MAKING MISSION HAPPEN

Curtis W. Dukes
Director, Information Assurance
National Security Agency

Who We Are: IAD

Protect Information – Outmaneuver Cyber Adversaries

- **Protect** systems that handle classified information, or are critical to military or intelligence activities
  - *National Security Information Systems, as defined in National Security Directive 42 (NSD 42)*
- **Advise and Support** Federal information security efforts
- **Support** private sector security

Confidence in Cyberspace

The State of Cyberspace

Adversarial Objectives

Trends and Focus

- Traditionally Trade Secrets
- Last Two Years shift to PII/PHI
- Brazen tactics including Destruction and Public Acknowledgement

Anatomy of an Intrusion

Attacker TTP's

- Gain Access
- Exploit Trust Relationships
- Maintain Persistence and complete bulk Exfiltration
- Degrade and Destroy

Lessons Learned

Root Cause is Poor Network Hygiene

- Network Mapping/Baselines
- Patch Management
- No Continuous Monitoring
- Disregard for Operations Risk Notices / IA Best Practices

Consequences

Cost of Defense vs Intrusion

- 7.7M – Global Cost of cybercrime
- 46 Days –to resolve a cyberattack
- 445B – Annual Cost to Economy
- Loss of Credibility Confidence
- Long term loss undetermined

Adversarial Objectives

Trends and Focus

- Traditionally Trade Secrets
- Last Two Years shift to PII/PHI
- Brazen tactics including Destruction and Public Acknowledgement

Anatomy of an Intrusion

Attacker TTP's

- Gain Access
- Exploit Trust Relationships
- Maintain Persistence and complete bulk Exfiltration
- Degrade and Destroy

Intrusion Lifecycle and Mitigations

Remote CNE Operator

PROTECTIONS PROVIDED BY THE IAD Top Ten Mitigations (Top Ten) and the Host Mitigations Package (HMP) (subset of Top Ten)

Reconnaissance

Collect target email addresses, scan servers for vulnerabilities

Enable Anti-Exploitation Features (such as EMET) (HMP)
Prevent malware from exploiting vulnerabilities

Take Advantage of Software Improvement (Top Ten)
Patch and upgrade to less vulnerable, better protected versions

Initial Exploit

Spear-phishing, water-holing, exploit known CVE, SQL injection, exploit zero-day vulnerability, etc.

Secure Host Baseline (SHB) (Top Ten)
Harden configurations to reduce vulnerabilities

Establish Persistence

Privilege escalate on local computer
Use "run keys", "scheduled tasks", "services" or other persistence points on Windows computer

Implement Application Whitelisting (HMP)
Restrict execution of programs (including malware)

Implement Host Intrusion Prevention System (HIPS) (HMP)
Restrain malicious behavior of malware

Install Tools

Backdoor implant or beacon for command and control (C2) and download modules
Use public services (e.g., Google, Twitter, Facebook) for C2

Use Anti-Virus File Reputation Services (HMP)
Block known and low reputation malware

Use DNS Reputation Services (Top Ten)
Restrict connections to low reputation sites

Move Laterally

Collect administrative credentials from Group Policy scripts or local machine using Mimikatz and other open source tools
Use pass-the-hash (PtH) and other methods to use stolen credentials to spread to other computers
Search for more privileged credentials (e.g., Domain Admin) to control entire network

Control Admin Privileges (Top Ten)
Prevent stealing admin creds

Limit Host-Host Comms (Top Ten)
Constrain lateral movement

Segregate Networks (Top Ten)
Limit spread

Collect, Exfil, Destroy Data

SAMPLE ADVERSARIAL TOOLS, TECHNIQUES, AND PROCEDURES (TTPs)

Use SSL, Tor, BitTorrent, and other encrypted anonymous protocols to hide exfil traffic
Use drivers and special malware to destroy data and render systems unusable and unrecoverable

Offline Backups, Thin Clients/Sandboxing (Other)
Prevent and restore from destruction

Lessons Learned

Root Cause is Poor Network Hygiene

- Network Mapping/Baselines
- Patch Management
- No Continuous Monitoring
- Disregard for Operations Risk Notices / IA Best Practices

Consequences

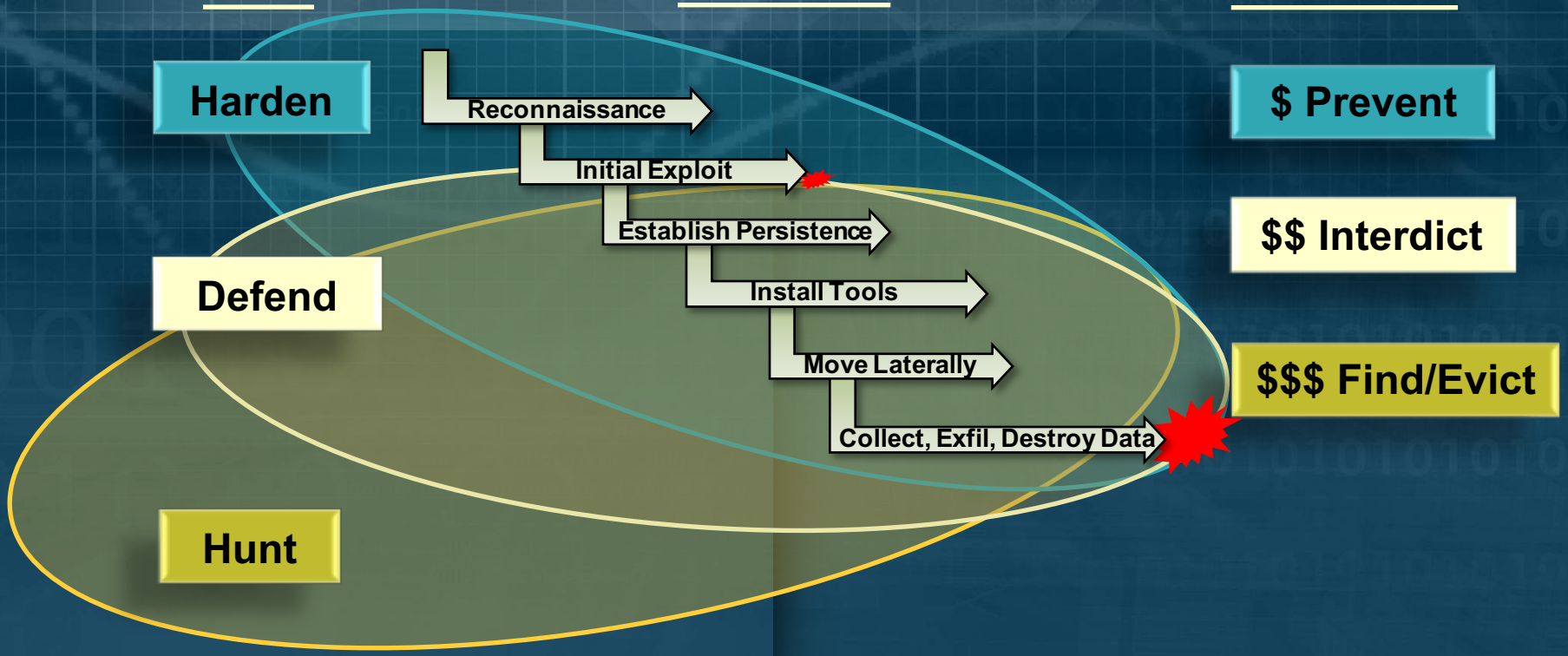
The annual cost of cybercrime to the

GLOBAL ECONOMY

is estimated at

$445 BILLION

What will we do about it?



Where to invest?

- Security as an executive suite priority with a resource loaded investment strategy.
- Funding identified in the IT budget for Information Assurance and network security.
- Future investments in tech refresh/network upgrades & architecture improvements.
- IA compliance mandated in contracting language and acquisitions.
- Continuous monitoring and measurable auditing of IT system for health & hygiene.

Questions?