

# The State of the Hack

Defending Your Organization in 2019

Mike Messick, President  
Deep Forest Security Consulting

# About Deep Forest Security

- Alaskan-based InfoSec Consulting Company
- Founded 2005, Blend of LE & F5 Experience
- Services
  - Information Security Risk & Vulnerability Management
  - Electronic Information Forensics
  - Incident/Intrusion Investigation, Response, & Remediation
  - ***Unified Security Management (new)***

# Current Threatscape

# Actors

Organized Crime



Nation-State



Botnet Hackers



# Techniques

- Initial Foothold
  - Phishing
  - Brute-Force
  - Browser Compromises
  - Social Engineering (BEC)
  - Zero-Day
- Assumes attackers can't get what they want directly from webserver database attack.





# Techniques

- Domain Access
  - Enumerate Hosts
  - Distribute Malware
  - Explore for Cool Stuff™
  - Disable Backups
  - Launch Ransomware
- If intelligence is end goal, then actors don't damage. They just steal. Barn is still on fire.



# Motivations

- Money
- Economic Espionage
- Impress Friends



# Motivations

- Money
- Economic Espionage
- Impress Friends
- Geopolitical Advantage



# Prevention

- Prevention Model Failed in Early 2000s
  - Flawed From the Beginning
  - Propagation of New Technologies Made It Worse
    - Cloud Hosting, SaaS, etc.
    - IoT Devices / “Smart” Things
  - Resulted in Ineffective Incident Response
- New Model: Detect & Contain



# Detect & Contain

- Plan for Intrusions To Occur
- Make Attacker Work Harder/Slower
- Be Able to See Attackers Quickly
- Limit Damage
- Recover From Attack
- Refine Strategy

# Mitigation Strategy

- Risk Analysis Drives All Mitigation Components
  - Most Organization Lag in Security Spending
    - Increased attack publicity is changing this
  - Security Mgmt. Program Maps Risks to Solutions
- Data Breach/Cyberattack Insurance
- Email Malware Scanning / Subject Prepending
- 2FA for External User Access

# Mitigation Strategy

- Limit Data Sharing for Partners via Firewalls
  - Limit Remote Access by IP
  - Limit Access to Internal Resources
  - DMZs when appropriate
- Default Outbound Deny FW Policy
- Redefine Backup Solutions
- Incident Response Plan



# Mitigation Strategy

- Network/System Visibility – Logs!
  - Infrastructure
  - Remote Access
  - Endpoints
- *Automated* Event Analysis, Correlation, Alerting
- Vulnerability Testing – External & Internal
- Network Traffic “Sniffing”

# Mitigation Strategy

- Network Intrusion Detection
- Web Traffic Malware Analysis
- Cloud Threat Intelligence Integration
- Training
  - Sysadmins / Security Admins – SANS, BlackHat, ShmooCon, etc.
  - Everyone – Phishing, BEC, Social Engineering



# Q & A

Mike Messick

Deep Forest Security Consulting

E-Mail: [mikem@deepforestsecurity.com](mailto:mikem@deepforestsecurity.com)

(907) 334-9090