



# Cyber Attacks: Adapting to the New Normal

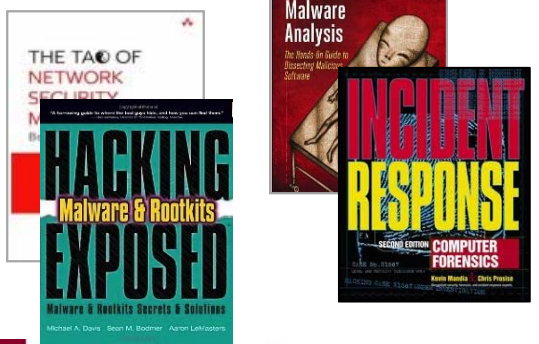
Email Sender & Provider Coalition

PRESENTED BY: John Foscue

MAY 2015

# Introduction

# Mandiant & FireEye: Experts in Advanced Targeted Threats



- **Expert Responders for Critical Security Incidents**
  - Incident responders to the biggest breaches
  - Our consultants wrote the book (literally) on incident response
  - Clients include more than 33% of Fortune 500
- **Full Range of Security Consulting Services**
  - Assessing & improving your security posture
  - Discovering and responding to security incidents
  - Developing your security programs, systems and processes
- **Worldwide Presence**
  - Mandiant is a FireEye Company
  - 2,000+ employees
  - Offices in 40+ countries



# Agenda

- Threat Landscape
- Initial Compromise – Attack Vectors
- Continued Fails
- Questions

The image features a central teal-colored horizontal banner with the text "Threat Landscape" in white. This banner is flanked by two vertical grey bars, one on the left and one on the right, which extend from the top to the bottom of the frame. The background is plain white.

# Threat Landscape

# Old Normal vs New Normal

It's a "Who",  
Not a "What"...

- There's a human at a keyboard
- Highly tailored and customized attacks
- Targeted specifically at you
- Effective at bypassing preventive controls

They are Professional,  
Organized & Well Funded...

- Generally a nation-state or organized crime
- Division of labor for different stages of attack
- Utilize change management processes
- Increase sophistication of tactics as needed











They are Relentless  
in Achieving their Objective

- They have specific objectives
- Their goal is long-term occupation
- Persistence tools ensure ongoing access
- If you kick them out they will return

***Organizations that do not fully understand this often react in ways that do more harm than good by tipping off the attackers.***

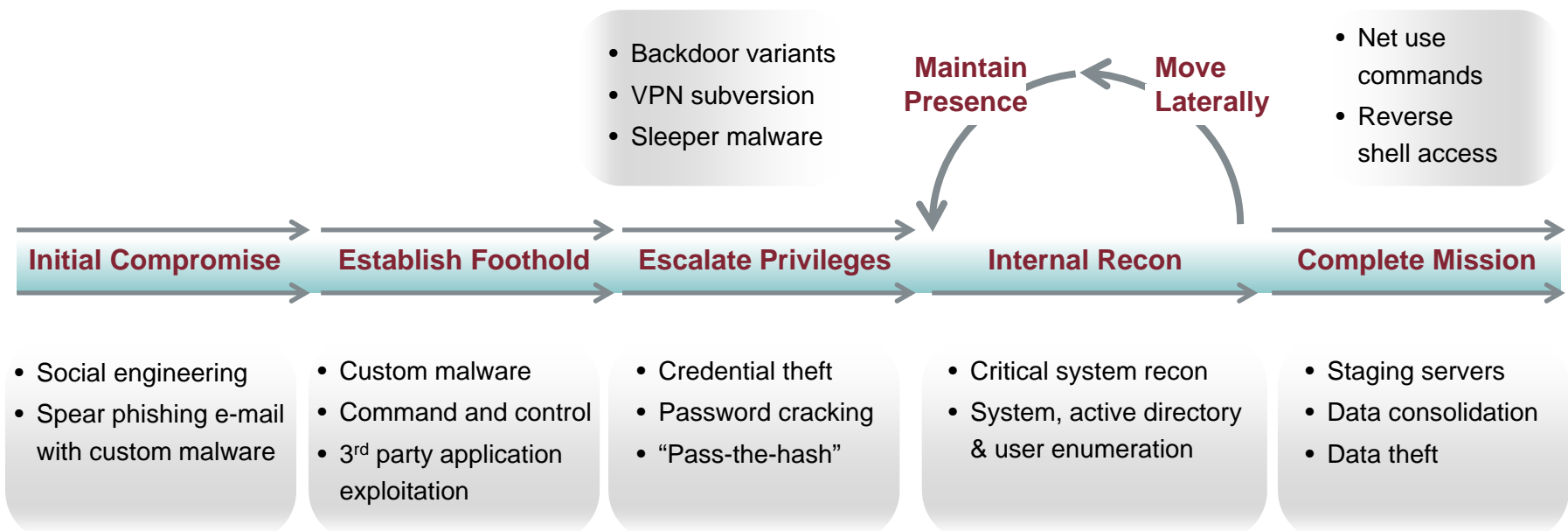
# Breaking Down the Threats



	<b>Nuisance</b>	<b>Data Theft</b>	<b>Cyber Crime</b>	<b>Hacktivism</b>	<b>Network Attack</b>
<b>Objective</b>	 <b>Access &amp; Propagation</b>	 <b>Economic, Political Advantage</b>	 <b>Financial Gain</b>	 <b>Defamation, Press &amp; Policy</b>	 <b>Escalation, Destruction</b>
<b>Example</b>	Botnets & Spam	Advanced Persistent Threat	Credit Card Theft	Website Defacements	Destroy Critical Infrastructure
<b>Targeted</b>					
<b>Character</b>	Automated	Persistent	Opportunistic	Conspicuous	Conflict Driven
<b>Origin</b>	Global	China Russia Middle East	Eastern Europe	Global	North Korea?

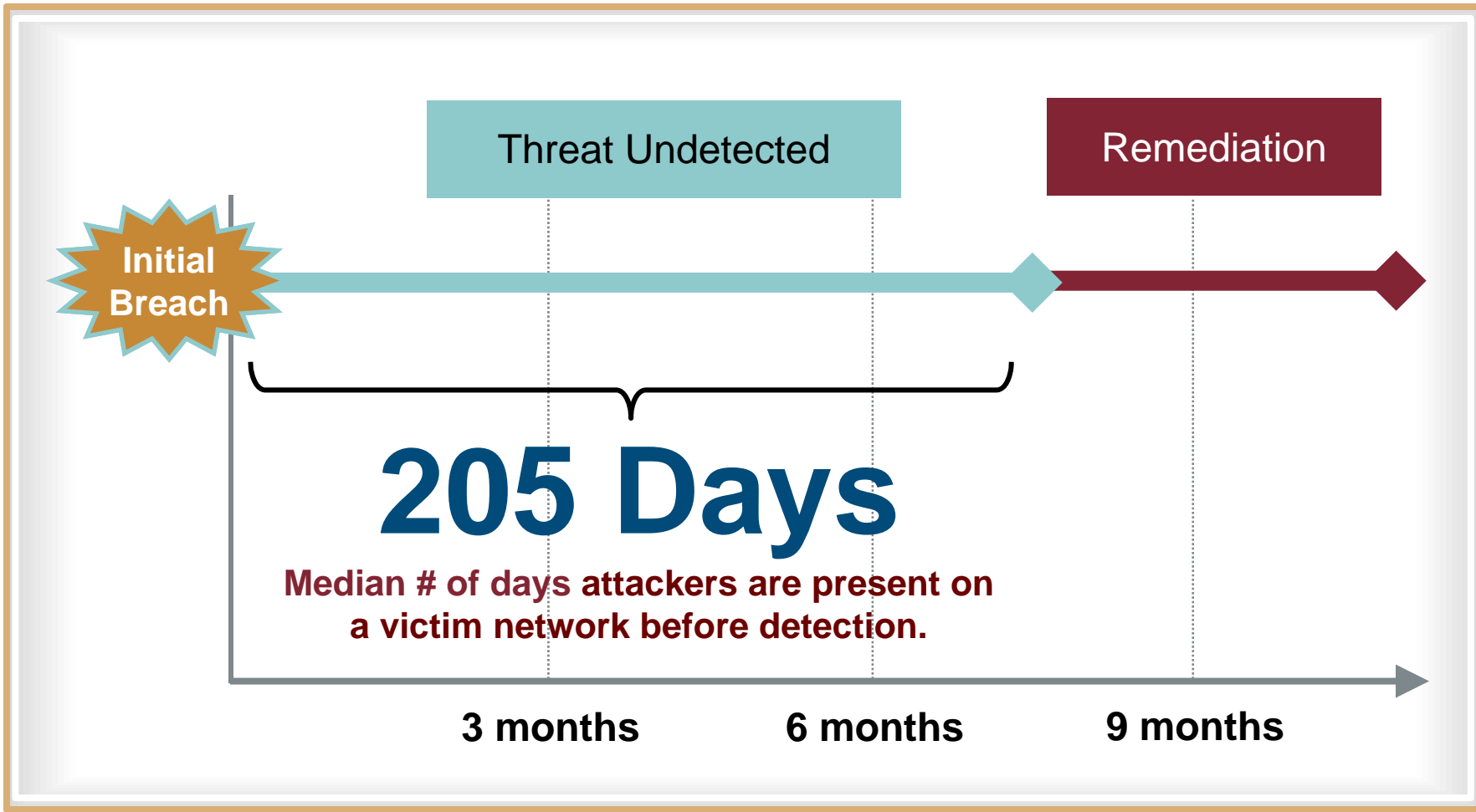
# Anatomy of a Targeted Attack

## Attackers Move Methodically to Gain Persistent and Ongoing Access to Their Targets





# The High Cost of Being Unprepared



**205 Days**  
Median # of days attackers are present on a victim network before detection.

Source: Mandiant M-Trends 2014



Initial Compromise

# Phishing Emails & Social Engineering



- Impersonating company employees
  - “Please install this security update software at the link below.”
  - From: [it-security@espcoa1ition.com](mailto:it-security@espcoa1ition.com)
- Impersonating other companies
  - “Thank you for submitting your resume. Please click this link for more information.”

# The Perfect Phishing Email

- Increase chances of success:
  - Sender Policy Framework (SPF) records
  - DomainKeys Identified Mail (DKIM) records
  - HTML based templates
  - Unsubscribe links
  - Linked payloads rather than attachments
- Decrease chances of success:
  - Spoofed email headers
  - Encrypted attachments
  - Sales oriented

What are companies still doing wrong?

# IT Security Fails

- Segmentation! Segmentation! Segmentation!
- No Multi-factor Authentication
- Email Signing and Encryption
- Patching Third Party Software
- Security Through Obscurity

A horizontal teal banner with the word "Questions?" in white text centered on it. The banner is flanked by two vertical grey bars on the left and right sides of the slide.

Questions?

# Contact Information



- John Foscue
  - [john.foscue@mandiant.com](mailto:john.foscue@mandiant.com)
  
- More MANDIANT info
  - [info@mandiant.com](mailto:info@mandiant.com)