PREPARED FOR REBOOT COMMUNICATION’S 18TH ANNUAL PRIVACY AND SECURITY CONFERENCE IN VICTORIA, B.C. (2/10/2017)

CYBERSECURITY IN 2017: PREPARING FOR THE ROAD AHEAD

MANDIANT®
A FireEye® Company

Presented by Marcus Troiano, Senior Cybersecurity Consultant at Mandiant, a FireEye Company

FireEye®
SECURITY REIMAGINED

Introduction

Responding to the most critical cybersecurity incidents and empowering organizations to protect their most critical assets.

THE TAO OF NETWORK SECURITY MONITORING
Practical Malware Analysis
INCIDENT RESPONSE
COMPUTER FORENSICS

- **Trusted Partner to Organizations Worldwide**
  - Clients include over 33% of Fortune 100 companies
- **Expert Responders to Critical Security Incidents**
  - Over 13 years experience responding to headline breaches
  - Renowned, published experts and true thought leaders
- **Assist With All Stages of Incident Response and Preparedness**
- **Global footprint with over 375 consultants in 20 offices across 5 continents**

The Threat Landscape of 2016

- **Acceleration of technological advancement**
  - Technology has changed how we communicate, how we do business, how we live - rapidly increasing attack surface
- **Explosion of public breaches and disruptive attacks**
  - Highest levels of business and government affected – all industries and all countries
  - Increase in state-sponsored politically motivated attacks, and ransomware and extortion
- **Improved Cybercrime tradecraft**
  - Attackers leveraged the latest technologies and innovative solutions
  - Few risks or repercussions, attribution is difficult
- **Heightened risk awareness**
  - Cybersecurity risk is getting Board and executive attention, no longer just an IT risk

Advanced Attack Targeting Motivators

CYBER ESPIONAGE

TARGETS THE DIB, **MILITARY** RESEARCH AND DEVELOPMENT ORGS, **THINK TANKS**, MFAs, AND **GOVERNMENT** AGENCIES

COMMERCIAL ESPIONAGE

PRIVATE INDUSTRY TARGETING DUE TO GOVERNMENT TIES AND **INTELLECTUAL PROPERTY**

DISRUPTION

DESTRUCTIVE ATTACKS THAT AIM TO DELETE INFORMATION AND/OR RENDER SYSTEMS **INOPERABLE**

CYBERCRIME

MOTIVATED BY **FINANCIAL GAIN** - PRIMARY MISSION IS TO STEAL INFORMATION THAT CAN BE **MONETIZED**

IT’S A “WHO,” NOT A “WHAT”

THEY ARE PROFESSIONAL, ORGANIZED AND WELL FUNDED

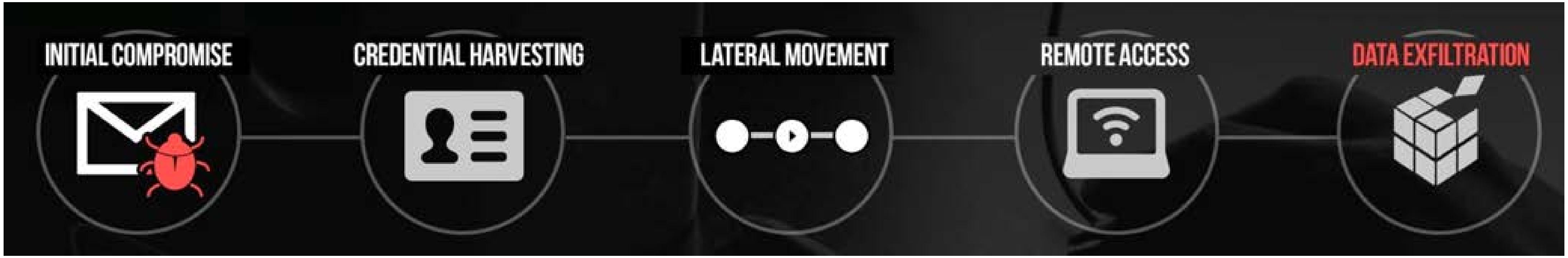
IF YOU KICK THEM OUT THEY WILL RETURN

MANDIANT®
A FireEye® Company

FireEye

Anatomy of an Advanced Attack

- Over 95% of attacks start with spear phishing campaigns



- Most organizations only realize they have been compromised when data has been stolen
  - On-average it takes 146 days for an attacker to be detected (469 in EMEA, 520 in APJ)

- Advanced attacks cost on average $4 million USD to deal with
  - They often take over a month to contain

100% of victims had firewalls and up-to-date anti-virus solutions

What’s Next in 2017?

- **Attacks will continue with increased sophistication and new targets**
  - More targeted and tailored ransomware and extortion attacks, affecting the mid-market
  - New threats for IoT, mobile, autonomous vehicles, and critical infrastructure
- **New legislation is coming, and the public is more engaged**
  - Canadian, EU, US cybersecurity policy and legislation updates
  - Greater level of accountability will begin to emerge
- **Endpoint visibility will remain a challenge**
  - Crowded playing field of next-gen endpoint agents leading to slow adoption
- **Difficult to attract and retain skilled resources**
  - Skill shortages will continue

How to prepare?

- **Validate that your cybersecurity capabilities are appropriate for the risks you face**
  - Understand where your crown jewels are, and how they are protected
  - Assess your cybersecurity posture and test your controls with red-team exercises

- **Embrace automation**
  - Automation and orchestration of response activities can help alleviate resourcing challenges

- **Establish relationships with key vendors and re-evaluate cyber insurance**
  - Having relationships with incident response, crisis management, and forensic firms is crucial
  - Re-evaluate your cyber insurance coverage – offerings have matured, and they deliver value

- **Intelligence-led security**
  - Transform your security operations with intelligence so you can adapt to the threat landscape

Additional Solutions: People, Process, and Technology

Identify sensitive data, move it to its own network

Ensures that attackers cannot easily move from one segment of the network to another.

Improve control over powerful accounts

Requires the most powerful accounts to be checked in / out prior to usage, usually protected by two-factor authentication.

“Dry runs” of incident response plan

Fewer than 20% of organizations test response plans with a cross-functional team on an annual basis.

Focus on phishing prevention

Phishing (luring users to click on malicious e-mail attachments) is still the #1 method that attackers use to compromise organizations. Most orgs are not well-protected.

Require two-factor authentication for remote access

Prevents attackers from using stolen passwords to access resources. Most companies prioritize remote access to e-mail and networks (virtual private networks).

Only permit pre-authorized programs to run on servers

Critical systems like servers generally only need to run a small set of software--yet they are often allowed to run arbitrary programs. “Whitelisting” technology can prevent this.

Use new technology to block advanced malware

New technologies can proactively execute and test web downloads in a secure environment (known as a “sandbox”) to find malware that traditional signature-based models miss.

Promote a “Security Culture”

Senior executives set the tone in any successful initiative. Security orgs often need increased support for new controls like two-factor access, incident response plan testing, etc.

MANDIANT®
A FireEye® Company

FireEye

THANK YOU

Marcus.Troiano@Mandiant.com

+1 647 885 0714