

M-TRENDS 2017

A View From the Front Lines

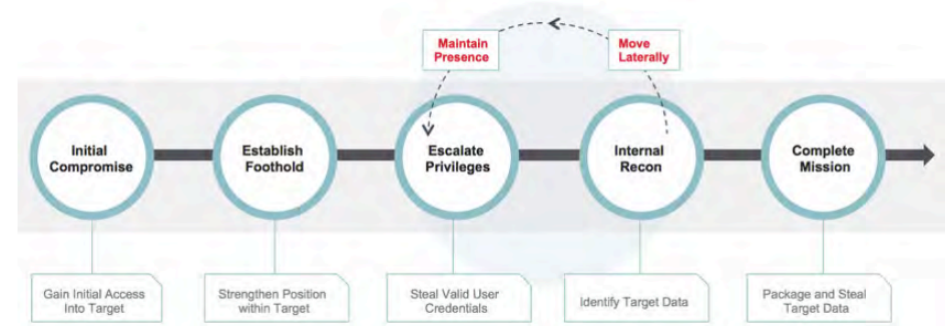
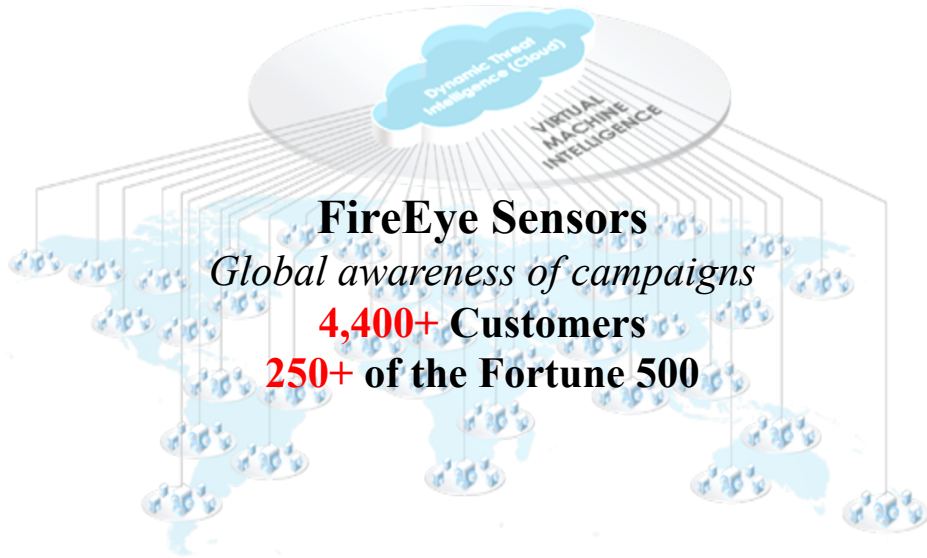


Introductions



Gerry Stellatos
Director, Incident Response
Gerry.Stellatos@Mandiant.com

Data is our Differentiator





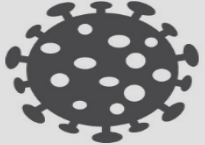







Agenda

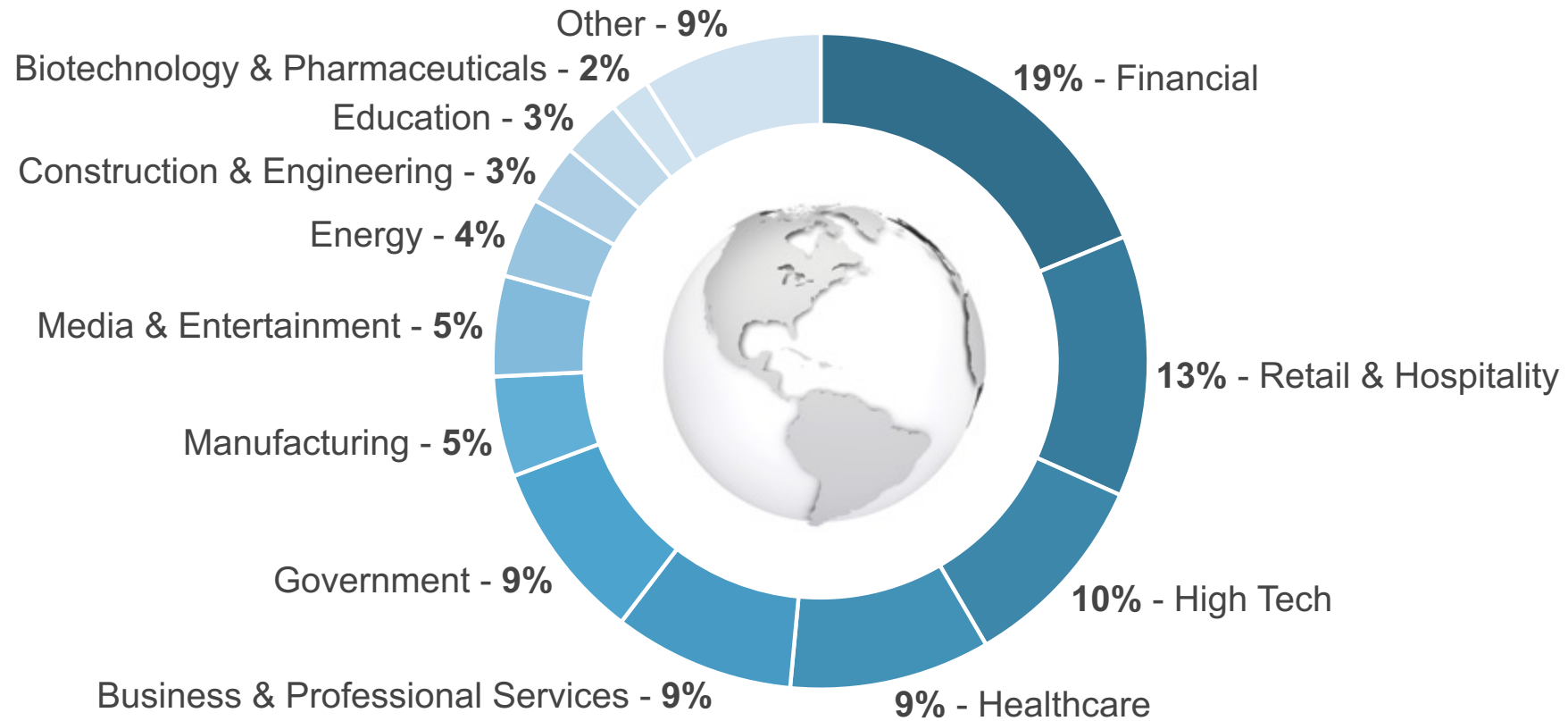
- By the Numbers
- Attack Trends
- Case Studies
- Questions



Threat Actor Motivations

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Disruption
Objective	 Access & Propagation	 Economic, Political Advantage	 Financial Gain	 Defamation, Press & Policy	 Escalation, Destruction
Example	Botnets & Spam	Advanced Persistent Threat Groups	Credit Card Theft	Website Defacements	Destroy Infrastructure
Targeted					
Character	Often Automated	Persistent	Frequently Opportunistic	Conspicuous	Conflict Driven

2016: Who's a Target

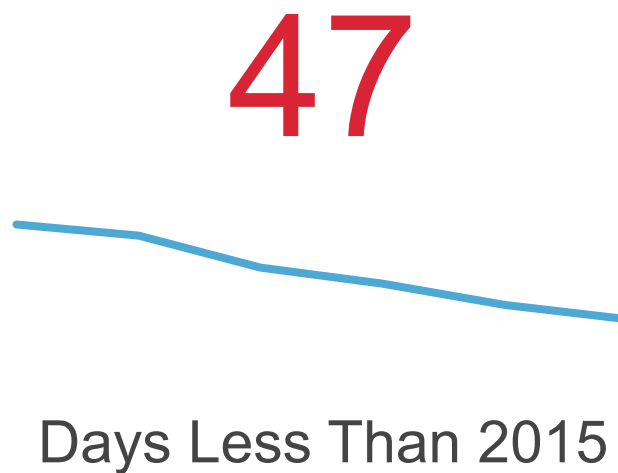


Other: Telecommunications, Transportation & Logistics, Nonprofit

2016: Dwell Time

99

DAYS



Detection
vs.
Dwell Time



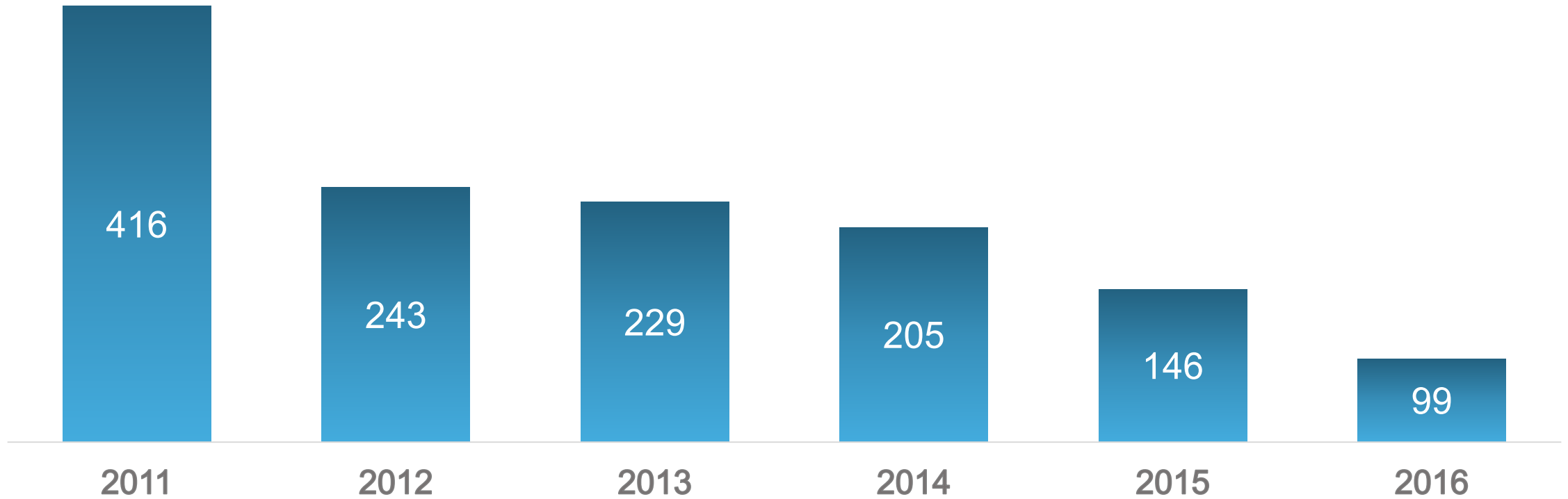
Internal:	80
External:	107

Breach to Discovery

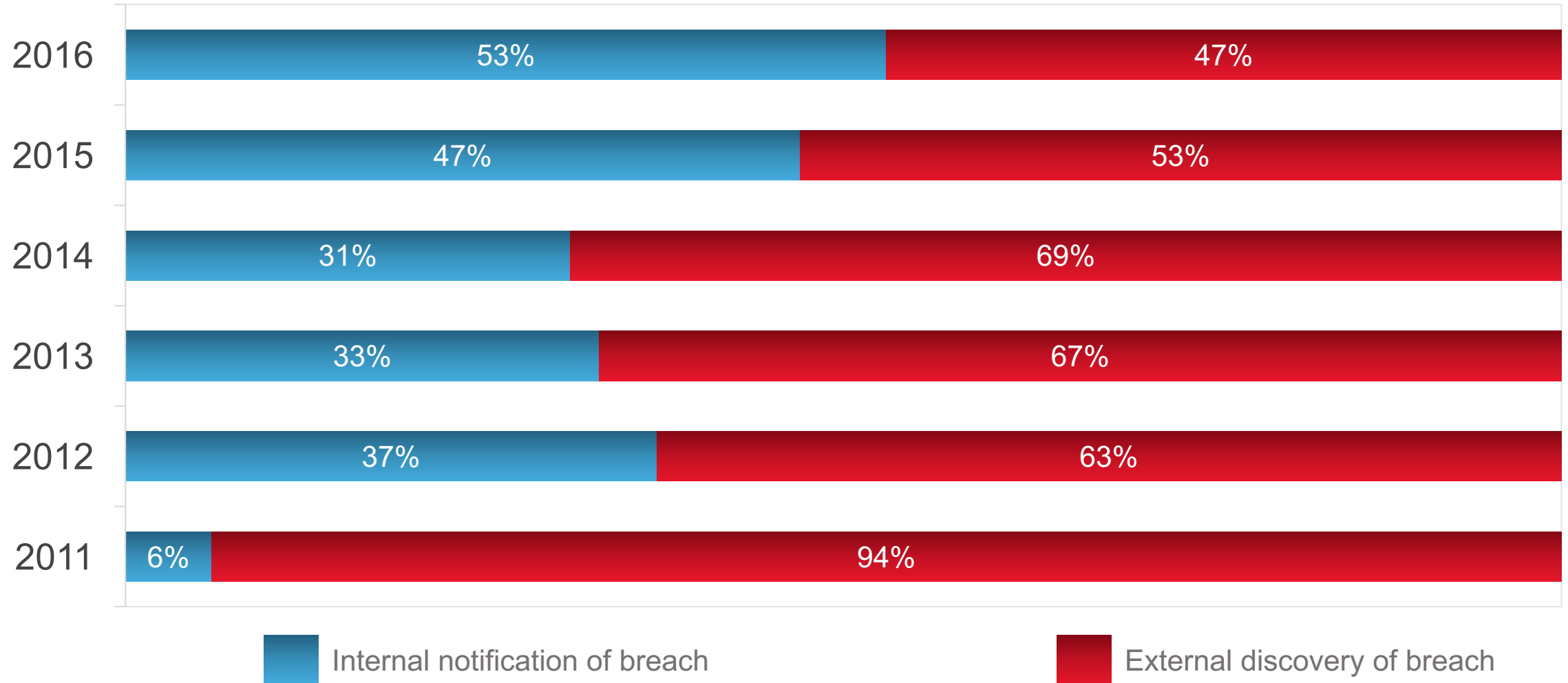
Median time from breach to discovery is getting shorter but still remains too long



M-TRENDS: Median Dwell Time



M-TRENDS: External Notification vs. Internal Detection



Attack Trends

Attack Trends

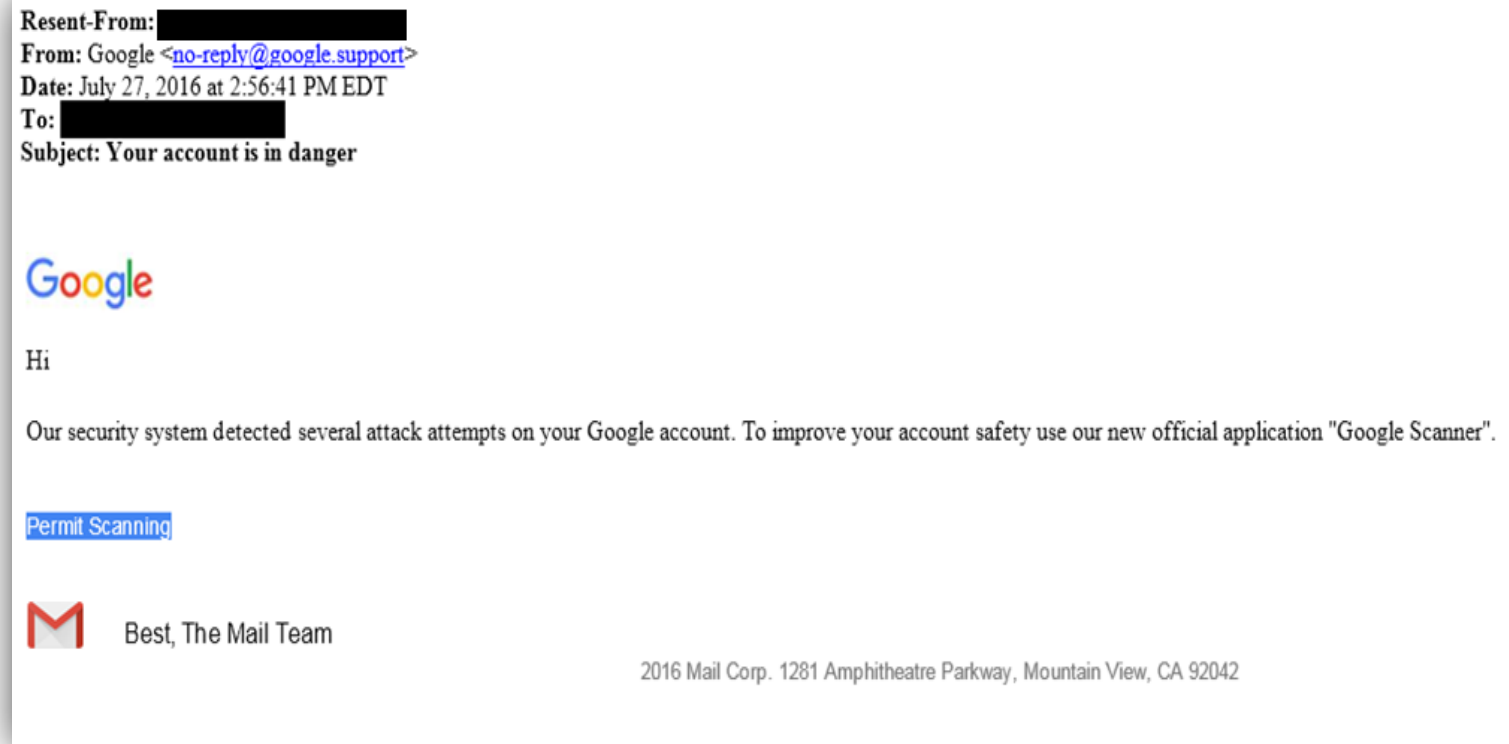
- Financial Crime - prior to 2013: “Unsophisticated”
 - Loud and straight-forward
 - Opportunistic
 - Rudimentary toolkits
 - (usually) Basic skills
- Since 2013, sophistication has been steadily increasing
 - 2014 M-Trends: “the lines are blurring between run-of-the-mill cyber criminals and advanced state-sponsored attackers”
 - Larger infrastructure, better toolsets, increased focus on persistence

Attack Trends

- 2016: “The line between the level of sophistication of certain financial attackers and advanced state-sponsored attackers no longer exists”
- Custom backdoors with unique, tailored configurations per target
 - Increased infrastructure resiliency
 - Counter-forensic techniques
 - Increased interest in inter-banking networks & infrastructure
 - ATMs

Attack Trends (cont.)

- Email has always been a major target
- 2016 showed an increase in interesting ways to access email

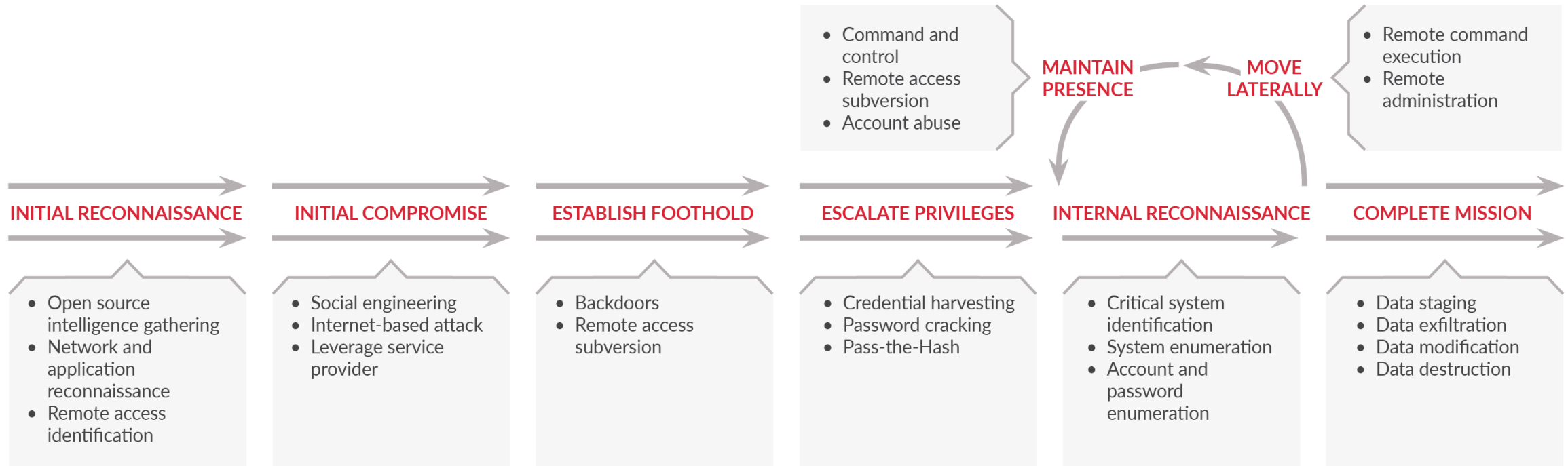


Attack Trends (cont.)

- Financial attackers tailor phishing email to specific client, location or employee
- Call victims to *help them*



The Attack Lifecycle



Adapting Foundational Defenses for the “New Normal”

- Not everyone is failing at detection and response
 - In 2016 multiple clients were successful at detecting and responding to Mandiant Red Teams
 - The best time so far against a Mandiant Red Team was 12 minutes
- Common themes
 - Small external threat surface
 - Robust endpoint controls
 - Skilled & empowered detection & response teams
 - Defined and tested detection and response playbooks

Industry Leading Practices

- Identification and protection of our most **critical assets**
- Annual “**red teaming**” of environments (internal and external networks, social engineering, and web applications)
- Requiring **dual factor authentication** on all remote access (VPN, Citrix, Terminal Services, and webmail)
- Deployment of **application whitelisting technology** to critical assets (domain controllers, mail servers, file servers, etc.)
- **Network compartmentalization** of critical assets and data
- Limit access to **system backups** to prevent intentional destruction
- Deployment of **advanced malware detection/prevention** technology at the perimeter (web and email)
- Searching for host and network-based **indicators of compromise** on a periodic basis
- Inventorying **privileged accounts** and resetting passwords on a periodic basis
- Leverage **threat intelligence** to facilitate risk assessments and enable incident detection and response

Thank You

Gerry Stellatos

Director, Mandiant Consulting

gerry.stellatos@mandiant.com