Introduction to Incident Response

Renana Friedlich, National Incident Response Leader
March 2016
Agenda

► Evaluation of Cybersecurity risks
► The attacker’s playbook
► Case study
► What can you do today
Evaluation of Cybersecurity risks

![Diagram showing the evaluation of cybersecurity risks with different attacker types and their associated motivations and tactics.]
Identity Theft Resource Center 2015 Survey

Data Breach Incidents - By Type

- Insider Theft
- Hacking / Skimming / Phishing
- Data on the Move
- Accidental Email / Internet Exposure
- Subcontractor / 3rd Party / Business Associate
- Employee Error / Negligence / Improper Disposal / Lost
- Physical Theft

Graph showing trends from 2007 to 2015.
Themes of most recent breaches

Following same “playbook” (no need to change):

► Gain access to internal company network
► Deploy RAT
► Obtain Windows “Domain Administrator” privileges
► Dump and crack password hashes of all corporate users
► Use cracked accounts to access sensitive data
► Extract data to a staging server
► Sell records when black market conditions are most favorable
“Lessons learned” from breach investigations

► PCI compliance ≠ difficulty in breaching payment cards
► PCI QSA audits did not test for current attack path
► Too many ways to get from corporate network to payment card network
► Protection of privileged service accounts
► Searches of security event logs take far too long to run (need more horsepower!)
► Breaches detected via external analytics vs internal monitoring capabilities
► “Blind” spots on network identified *after* breach
Notional attack timeline

1. Day 1
   - Company A sends email to victims

2. Day 1
   - Attacker blocks all emails from Company B to victims Gmail account

3. Day 2
   - Attacker sends wire request to fake email account

4. Day 2
   - Wire transfer

5. Day 5 2016
   - Company B validates wire request and transmits funds

   - Company A
   - Gmail

   - Yahoo!

   - Company B
   - Domain

   - Bank
Lessons learned

► Money transfer procedure
► Two-factor authentication
► Create e-mail rules
► User awareness training
## What can you do today?

<table>
<thead>
<tr>
<th>Section</th>
<th>Actions</th>
</tr>
</thead>
</table>
| **Know your critical assets** | ▶ Identify the “crown jewels” of your organization  
▶ Understand the data flows and assets that store, process and transmit the data  
▶ Inform your security operations team of the critical assets’ priority |
| **Assess your logging capabilities** | ▶ Leverage Center for Internet Security and vendor benchmarks to assess logging devices on critical assets  
▶ Determine whether other tools are required for enhanced logging |
| **Privileged and remote account management** | ▶ Monitor, monitor, monitor the keys to the kingdom  
▶ Remove local administrator access from users!  
▶ Re-assess all remote accounts and whether any access is through single-factor authentication |
| **Build your IR plan, templates and tabletop** | ▶ Build a comprehensive IR plan leveraging industry publications  
▶ Build communication emails and other templates that help provide a consistent IR experience  
▶ Conduct IR tabletops using real-life scenarios. Consider inviting external partners (e.g., FBI) to participate |
“There are only two types of companies: those that have been hacked, and those that will be.”

Robert Mueller, Former FBI Director
Thank you

Responding to Targeted Cyberattacks

http://isaca.org/cyberattacks

2015 Global Information Security Survey

http://www.ey.com/GL/en/Services/Advisory/EY-cybersecurity

Renana Friedlich
Los Angeles, CA
Phone:  +1 213 977 3928
E-Mail: Renana.Friedlich1@ey.com