Today’s Presentation

1) Overview of Cyber Threats
2) Current Approach to Cyber Risk Management
3) Challenges with the Current Approach
4) The Role of Threat Intelligence
5) Countering Advanced Adversaries
Cyber Threats – Who is trying to take us down today?

- **Where Is The Adversary?**
  - China (Asia Pacific)*
  - Russia (Eastern Europe)*
  - Middle East*

- **What Do They Want?**
  - **Specific Sectors**
    - Healthcare, Pharmaceuticals, Financial Services, & Defense
  - **Specific Information**
    - Personal Identifiable Information (PII), Account Numbers, Intellectual Property, & Financial Reports,
  - **Specific People**
    - Executives, Senior Leadership, Legal Departments, Human Resources, Researchers, & Executive Assistants

- **High-Level Methodology**
  - Obtain Information From Public Facing Sites and Documents
  - Leverage Social Engineering and Spear-Phishing Tactics
  - Establish Strong Foothold Through Multiple Backdoors
  - Slow Exfiltration Of Data From Your Network To Theirs
  - Remain Persistent and Anonymous Throughout the Process

*Note: Not an exhaustive list of adversaries, but rather where most attacks originate from according to industry reports
The rise of compromise from insiders who conduct data breaches and create even greater liability for an enterprise

The Insider Threat

<table>
<thead>
<tr>
<th>Category</th>
<th>No. of Financial Institutions Reporting Repeated Occurrences of Internal Data Breaches in Last 12 Months</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidental</td>
<td>39</td>
</tr>
<tr>
<td>Malicious Software</td>
<td>35</td>
</tr>
<tr>
<td>Malicious Insider</td>
<td>28</td>
</tr>
<tr>
<td>Financial Fraud</td>
<td>14</td>
</tr>
<tr>
<td>Internal Breach</td>
<td>11</td>
</tr>
<tr>
<td>Non-Employee</td>
<td>7</td>
</tr>
<tr>
<td>Third Party Vendor</td>
<td>7</td>
</tr>
<tr>
<td>Mobile</td>
<td>4</td>
</tr>
</tbody>
</table>

Case Study: Julian Assange’s WikiLeaks is an enabler for insiders to anonymously expose your firm’s most sensitive intellectual capital, trade secrets, and proprietary & confidential data

- Ex: Bank of America, US State Dept. (Diplomatic Cables)
- 33% of 900 data breaches in a six-year study were in the financial services industry; the industry also accounted for a staggering 94% of compromised records

Only 34% of survey respondents said they were “very confident” about being protected against internal attacks

Booz | Allen | Hamilton
The current approach to addressing advanced threats is failing – over and over and over and over!

<table>
<thead>
<tr>
<th>Advanced Threats</th>
<th>Common Countermeasures</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Leakage – Social Media / Insider Attacks</td>
<td>Network Restrictions; Security Policies; and Data Loss Prevention (DLP)</td>
<td>Insiders Seem to Always Find a Way!</td>
</tr>
<tr>
<td>Social Engineering &amp; Spear Phishing</td>
<td>E-Mail Filters; User Awareness Training</td>
<td>Well-Executed Attacks Yield a 90% “Kill Ratio”</td>
</tr>
<tr>
<td>Software-based Advanced Persistent Threats (APTs)</td>
<td>Network and System Monitoring; Network Segregation</td>
<td>High Degree of Difficulty and Expensive; Users “Go Rogue”</td>
</tr>
<tr>
<td>Advanced Hardware Attacks</td>
<td>Network Monitoring, Drive Encryption, and Physical Controls</td>
<td>State-Sponsored Attacks can be Extremely Skilled</td>
</tr>
</tbody>
</table>
Heavy investments in traditional countermeasures have helped, but fail to address advanced threats

### Traditional / Common Defenses

- **Anti-Virus:**
  - Signatures Detect Only 25% of Advanced Malware
  - Adversary Uses Encryption and Obfuscation
  - Utilization of Unknown Vulnerabilities (Zero Day)

- **Intrusion Prevention / Detection:**
  - Skilled Attackers Evade Signature and Detection
  - Traffic and Tools Are Often Encrypted
  - Lateral Attacks Evade Detection

- **Firewalls & Filters:**
  - Destination IP Addresses Change
  - Use Common Ports Such As 80 and 443
  - Content Appears to Be Legitimate
  - Source Addresses Changes Frequently

- **DLP & User Training**
  - Requires Strict Data Classification & Categorization
  - Rogue Users and Malicious Insiders
## Background

- Multiple executives were travelling overseas in support of a key technology conference
- Ten brought along laptop computers for day to day use during the conference
- Laptops were secured in hotel room safes while not in use (according to the users)
- Full drive encryption was used to protect data at rest on all laptops
- VPN protected all communications to/from cooperate assets

## Challenge / Compromise

- Upon returning to the US and connecting the corporate networks **anomalous network traffic was observed** from 2 laptops
- Analysis revealed **encrypted/encoded communications with servers overseas**
- Suspected systems were quarantined and examined
- **Network drivers had been modified**
- 6 laptop computers have been physically tampered with and **unknown ICs were installed**

## Lessons Learned

- Laptop computers can be compromised even with full drive encryption enabled
- Do not permit laptops with sensitive data to be taken overseas
- Quarantine and examine laptops returning from overseas trips
- **It is impossible to restrict/control all laptops – controls must be targeted to high risk assets**
### Background
- Recent data breach and subsequent exposure led to “recruitment drive” of insiders at a Fortune 100 client
- Public statements indicated an imminent data leakage event
- Public statements indicated one or more well positioned insiders as sources for leaked data

### Challenge / Compromise
- Unknown attack vectors could be used for data exfiltration
- Serious challenges in identifying top executives and staff with data access
- Massive enterprise footprint to defend with hundreds of network ingress/egress points
- Large number of personnel and staff
- No operational knowledge of the adversary

### Lessons Learned
- It is imperative to know where you sensitive data is, and who can access it
- Highly enhanced security controls fail across an entire enterprise – too expensive!
- A **detailed understanding of the adversary** enabled real-time security control enhancements
- Identifying the individual adversary allowed for **targeted legal action**
# Case Study: Imminent DDoS Attacks

## Background
- A major client was under near term threat of a massive DDoS attack
- Unknown group of adversaries
- Unknown Tactics, Techniques and Procedures (TTPs) for attack
- Unknown attack history / understanding of previous events

## Challenge / Compromise
- Amorphous community of loosely-banded threat actors and hacktivists targeting network infrastructure
- Massive client organization offered wide-spread attack surface to would-be attackers
- Disruption of client systems would result in significant nation-level transportation interruptions

## Lessons Learned
- Identifying TTPs in advance of an attack makes responding much easier
- Early engagement with service providers and infrastructure staff enables a rapid response
- Advanced warning of attacks with details on likely TTPs enables proactive action
- Addressing the challenge proactively eliminated any significant impacts
What does “Threat Intelligence” really mean?

- A dedicated program focused on collecting data on current and emerging adversaries
  - Know your enemy!

- Often leverages data source both internal and external to the organization

- Enables a dynamic approach to cyber security risk management

- Limits heavy investments to the highest risk areas
Remediating the risks posed by advanced adversaries across a huge enterprise is cost prohibitive
- Protecting ALL of your data = impossible
- Monitoring ALL of your people = impossible

Enhanced controls must be selectively applied based upon detailed knowledge of current/emerging threats

Building a threat intelligence program is extremely challenging
- Still viewed as a technology problem with the inevitable quest for a “silver bullet” solution
- Requires a heavy mix of people skills – Intel analysts are not easy to come by!
- Mandates a different approach, one encompassing people, process, and technology – all working together
Threat Intelligence – Success Criteria

- A risk aligned program that is right-sized for your organization
  - No one-size-fits all solutions
  - Focuses on threats that are currently impacting your sector/organization – or will in the near/mid future

- Compliments a mature risk management and security program

- Program produces actionable outputs and reports
  - An information/awareness based program is interesting, but of little practical value
  - Does your organization make positive changes based upon threat intel and reports?
Threat Intelligence – Major Program Components

Collection
- Mix of internal and external data feeds
- Data vetting and storage

Production
- Define consumer requirements
- Aggregation
- Analysis

Wargaming & Exercises
- Evaluate risk posture vs. threats
- Assess impacts with threat informed wargames / exercises

Stakeholder Communications
- Disseminate intelligence reports
- Engage with “customers” to monitor requirements
Blueprint Your Program

Roles & Requirements

- Insourced vs. Outsourced
- Links to internal and external data
- People, Process and Technology

People are the key to success
- Define appropriate roles and responsibilities

Training & Development
- Develop the right skills
- Attract the right staff
- Work more efficiently
Threat Intelligence – How to Begin or Evolve?

- **Evaluate your current program or your current needs**
  - How do you compare to an industry leading threat intelligence program?
  - How actionable and relevant are your threat reports?
  - Is your data safer today because of your current program?

- **Design a right-sized program**
  - May be a mix of in/outsourced services
  - Consider developing a holistic program blueprint laying out the people, process, and technology layers to the solution

- **Focus on people skills**
  - The skill of your intelligence analysts will make or break your program
  - Focus on a mix of skills ranging from pure data analytics to cyber technical skills – and all points between
Questions & Contact Information

What did we NOT talk about?
Questions?
Comments?
War Stories?