Social Engineering: How an Employee’s Digital Footprint May Tread on His Employer

by Craig Guiliano, Director of Security Solutions
TSC Advantage Philosophy

- External Business Operations
- Insider Threat
- Data Security
- Internal Business Operations
- Physical Security
- Mobility
Agenda

• Insider Threat
  • What is an Insider Threat and Why is it important?
  • Types of Insider Threat
  • Stats and Case Studies

• Social Engineering
  • What is it? Why does it matter?
  • Scoular: Case Study

• Phishing VS Spear Phishing
  • What is it?
  • Anatomy of Phishing Attacks
  • Recent Examples

• “Operation Ox”
  • Social Engineering Experiment
2013-2016
Social Engineering and Insider Threats

17,642 Victims
270% increase in victims
Over $2.3 billion in losses
+50% of employees would steal & sell trade secrets

Source: FBI
WHAT is an Insider Threat?

Current or former employee, contractor, etc. who has/had AUTHORIZED access to the network, system, or data.

WHY does it matter?

Upwards of 70% of all cyber breaches are attributed to a credentialed insider and NOT a remote attack.
TYPES of Insider Threats

**Negligent Insiders** - Insiders who accidentally expose data – such as an employee who forgets his/her laptop on an airplane

**Malicious Insiders** - Insiders who intentionally steal data or destroy systems – such as a disgruntled employee who deletes some records on his last day of work

**Compromised Insiders** - Insiders whose access credentials or computers have been compromised by an outside attacker
WHO are the perpetrators?

Approximately 1/3 of all cases are for the benefit of a foreign government or company.

WHO is at risk?

Anyone with access to data, networks, computers, mobile devices, IP etc.
Insider Threat

**HOW can it occur?**

Recruitment through Social Engineering, Phishing, Dumpster Diving

**WHEN does it occur?**

Majority of insiders strike during normal hours using authorized access or within two weeks of a significant personnel action (firing, demotion, resignation, promotion)

**Tactics, Techniques & Procedures:**

Elicitation, Cold Pitch, Social Engineering, Exploiting Vulnerabilities, etc.
Social Engineering

Adversary uses human interaction + social skills to obtain or compromise sensitive data

Use of Cover:
• An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity

Pretext Phone calls:
• Use of elicitation techniques to collect seemingly innocuous data + or in conjunction with email

Pieces of a Puzzle:
• All data is intelligence to support sophisticated attacks
• Criminals impersonated the Scoular CEO and a KPMG partner by creating phony email accounts and spoofing phone numbers

• Using these phony email addresses & numbers, the criminals convinced Scoular financial advisor to send $17.2 million to an offshore account

• Complex combination of international resources (servers, email addresses) located in China and Russia, among others

Similar schemes netted $800 million in the past six months

**Email from (phony) CEO to Scoular’s CFO**

“We need the company to be funded properly and to show sufficient strength toward the Chinese. Keith, I will not forget your professionalism in this deal, and I will show you my appreciation very shortly.”
Phishing:
• Exploratory attacks targeted at a broad audience.
• A combination of social engineering and technical deceit
• Goal: to manipulate victims into opening file attachments or clicking on embedded links in an email

Spear Phishing:
• Much more sophisticated and elaborate
• Targets a SPECIFIC individual, organization or entity
• Goal: Coerce a HIGH VALUE target into opening an attachment or clicking an embedded link

Cross Site Scripting:
• Code injection attack into a victim’s browser
• Popular attack used in phishing campaigns
• Goal: to execute malicious Javascript.
Recent Spear Phishing Example

Attachment exploits specific vulnerability in MS Word

Appears to come from a legitimate contact at the Ministry of Defense.

Context: India has provided significant aid to Afghanistan. Recipient Indian Ambassador to Afghanistan

Source: Palo Alto Networks
## 5 C’s of Cyber

<table>
<thead>
<tr>
<th>CATEGORIES</th>
<th>DESCRIPTION</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convenience</td>
<td>Attacks against open vulnerabilities</td>
<td>Company with open ports, unencrypted data</td>
</tr>
<tr>
<td>Circumstance</td>
<td>Threats introduced via business dependencies</td>
<td>Suppliers with vulnerabilities or are high-value targets</td>
</tr>
<tr>
<td>Consequence</td>
<td>Specific high-target and high-value industries</td>
<td>Banking, retail, healthcare</td>
</tr>
<tr>
<td>Conflict</td>
<td>Military, political, terrorist and nation-state targets</td>
<td>Critical infrastructure</td>
</tr>
<tr>
<td>Conscience</td>
<td>Protesters or “hacktivists”, motives are cause vs financial gain</td>
<td>Ashley Madison</td>
</tr>
</tbody>
</table>
Where Do You Fit?

Convenience

Circumstance

Conflict

Consequence

Conscience
Objective: Conduct a cyber operation against a conference attendee to target his/her company

- Immediate Task: Gather as much intelligence on the target as possible

- Secondary Task: Conduct concerted spear phishing campaign using data collected during recon to exploit company network

- Tertiary Task: Do not get arrested
Conduct Initial Background and Intelligence Gathering

- Identify social media presence, employment history, family, etc.
- Cognizant of potential motivations or vulnerabilities to exploit

Relationship building (Linked In/Facebook/Events)

- Connect through social media and professional associations
- Begin to establish “cover” to make initial contact based on the target’s profession, hobbies, etc.

All of this provides a pretext for direct contact…
What information is out there?

[Logos of Instagram, LinkedIn, ARACHNYS, Spokeo, Experian, DiscoverOrg, Intelligroup]
Preparing for the Campaign

What did we discover? Gap Analysis…

- Education history, family, background, professional relationships
- Company information and potential supply chain vulnerabilities
- Important contact information to begin planning social engineering exploitation and spear phishing campaign

How does this information increase the likelihood of our success?

- Craft tailor-made “emails” that appeal to the target (think Indian Ambassador).
- Use contact information and travel updates to our advantage in gathering more intelligence for additional attacks and social engineering
Creating the Attack

```
postfix/qmgr[8265]: 5B1D940989: from=<it@crain.com>, size=10687, nrcpt=1 (queue active)
postfix/smtpd[9600]: disconnect from localhost[127.0.0.1]
postfix/smtp[9605]: 5B1D940989: to=<poxner@businessinsurance.com>, relay=bus
businessinsurance-com.mail.protection.outlook.com[207.46.163.138]:25, delay=2.8, delays=0.05/0.01/1.7/1, dsn=2.6.0, status=sent (250 2.6.0 <20160310190538.5B1D940989@ > [InternalId=75058848466084 , Hostname=C01PR07MB848.namprd07.prod.outlook.com] 16162 bytes in 0.406, 38.828 KB/sec Queued mail for delivery)
postfix/qmgr[8265]: 5B1D940989: removed
You have mail in /var/mail/
```

```bash
:~/var/log$
```
Hello,

The IT department is tracking issues with viruses and other malware spreading throughout many Crain and BI hardware assets.

Attached is a spreadsheet showing affected staff and computers. Please open and view the contents. If you see your name on there, please contact the IT department as soon as possible for remediation and next steps.

Thank you,

James Franken
Systems Engineer
Crain Communications
it@crain.com

Crain Communications Ltd
And...Confirmation

Date/time of successful execution

Work email address targeted to exploit network
Find what's next and see how far you can go.
Inspiring creativity and innovation

San Jose State provides one of this nation's highest quality, accessible, affordable, and leading-edge educational programs in art and design.
Summary

Real Nature of Cyber Threats
• Cyber security is hardly a technology-only problem
• Increasing IT budgets and ignoring the human factor is not the answer

Ease of Targeting
• Yes, this could have been ANYONE and ANY COMPANY in this room
• Minimal time and effort to pull off an attack of this nature

What’s the answer? Proactive, holistic approach to cyber security that promotes the harmonization of technology, processes, and people.

✓ Training and Awareness
✓ Incident Response and Post-Breach Recovery
✓ C-Suite/Board Champion
Questions?

Craig Guiliano
cguiliano@tscadvantage.com