RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

When the Phone is More Dangerous than Malware

SESSION ID: HUM-R02

Christopher Hadnagy
Chief Human Hacker
Social-Engineer, Inc.
@humanhacker

Michele Fincher
Chief Influencing Agent
Social-Engineer, Inc.
@SocEngineerInc

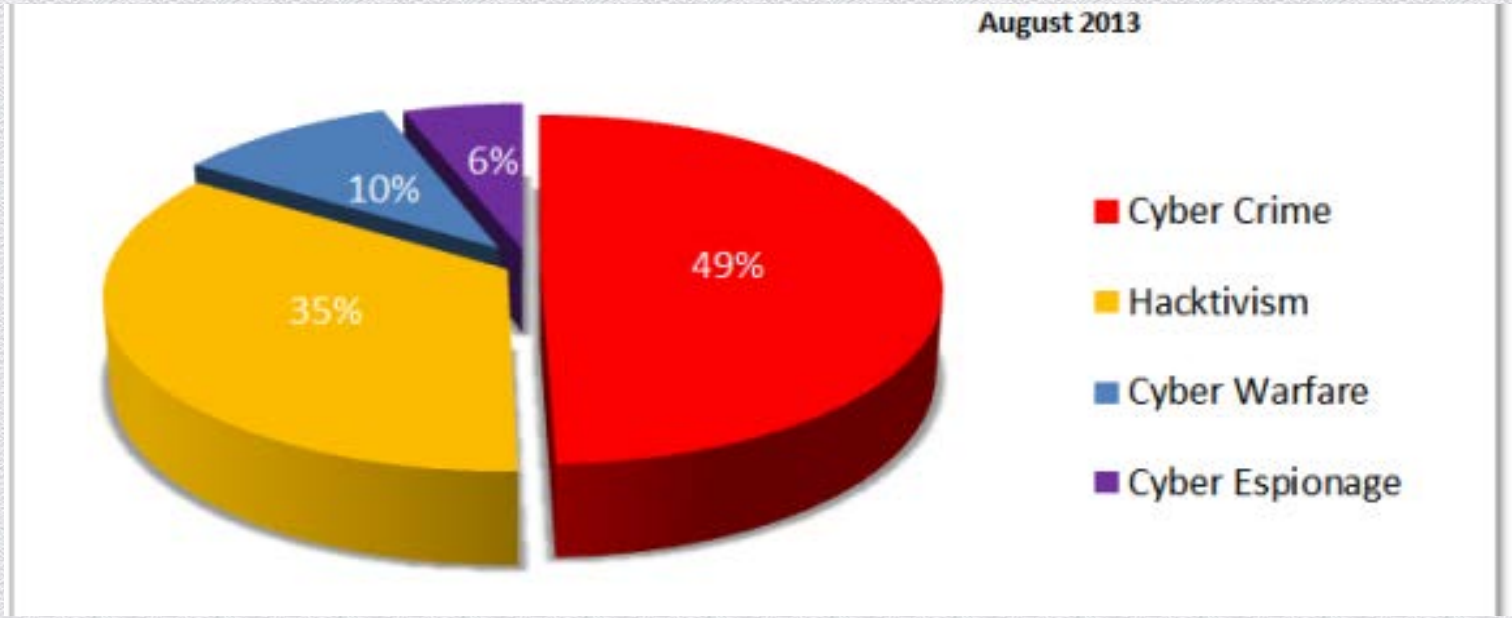
What is Social Engineering?

"….any act that influences a person to take an action that may or may not be in their best interests…"

What is a Social Engineering Attack?

- There are three main methods used in social engineering:
  - Phishing
  - Phone elicitation
  - Onsite impersonation

Scary Statistics & Quotes



Source: http://hackmageddon.com

Scary Statistics & Quotes

“Human errors and systems glitches caused nearly two-thirds of data breaches globally in 2012, while malicious or criminal attacks are the most costly everywhere at an average of $157 per compromised record.” - *2013 Cost of a Data Breach: Global Analysis*, Ponemon Institute and Symantec, June 2013

Scary Statistics & Quotes

“Through 2016, the financial impact of cybercrime will grow 10 percent per year due to the continuing discovery of new vulnerabilities.” - G*artner Top Predictions for 2012: Control Slips Away*, Gartner, December 2011

What Can You Do?

- Three-step process for successfully combatting social engineering
  - Be educated
  - Get regular check ups
  - Create critical thinking infrastructure

Step 1: Be Educated

- Learn to identify current SE Attacks
- Learn:
  - what to do IF an attack occurs
  - what to do WHEN they click/answer/let someone in
  - WHY malicious people use these types of attacks
- Learn how to effectively communicate risk to your staff
- Remember that technology cannot fix this problem

Step 2: Get Regular Check Ups

- A company can't fix problems they don't know exist
- Don't go with the "free clinic", but a specialist
- Identify the risk, test the vulnerabilities and work on patching
- Educate without fear
- Re-test

Story Time

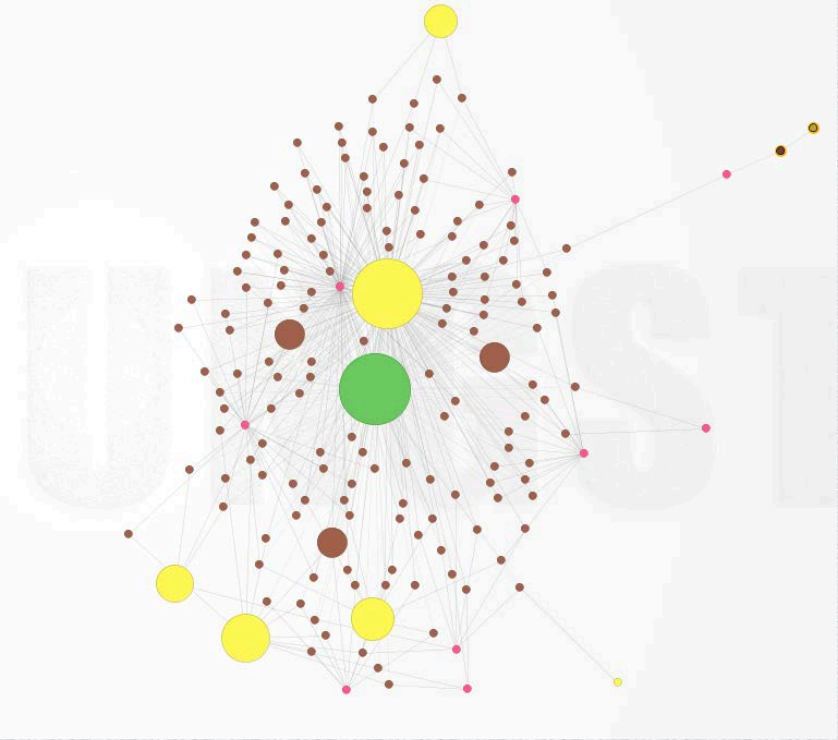
Step 2: Story Time

Step 2: Story Time

They wanted to test their company against an all-out social engineering attack that would utilize:

- Phishing – 2 campaigns at varying levels
- Spear phishing of every executive
- Phone elicitation against a section of each department
- Physical entry access to 4 of their main buildings

SE Pentest Stage One: Info Gathering



- Corporate website
- Google dorks
- Company browser websites
- Vendors
- Review sites

And of course…

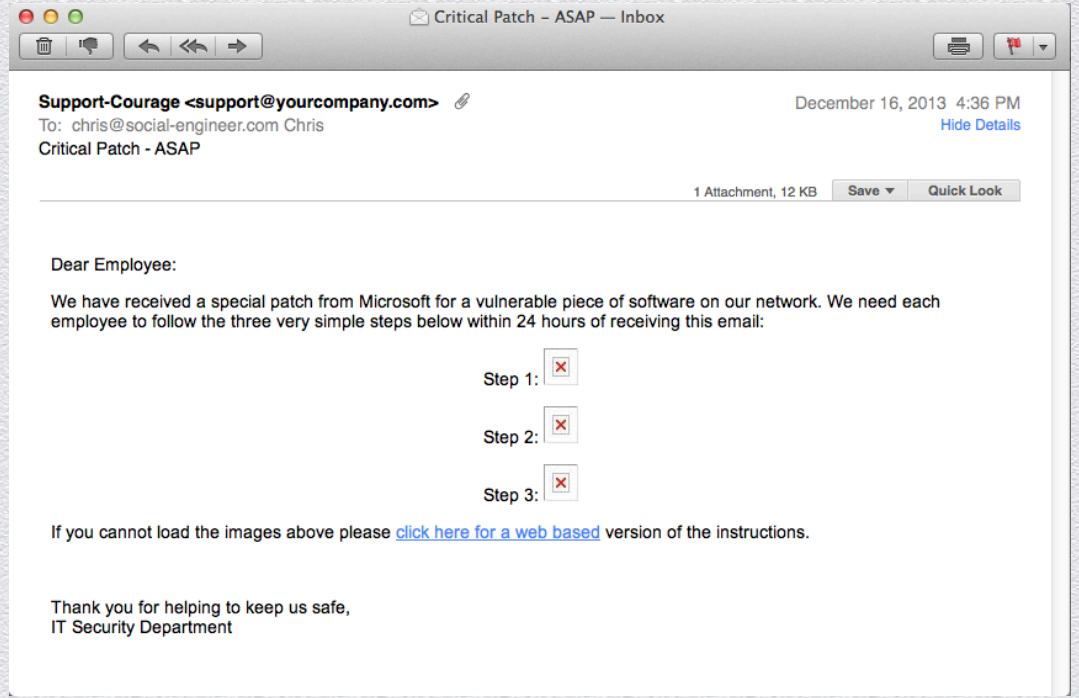
- Social media

SE Pentest Stage Two: Profiling

Goal in this stage:

- Determine culture
- Specific vulnerabilities
- Hobbies / likes / dislikes
- Email methodology
- Policies for information release

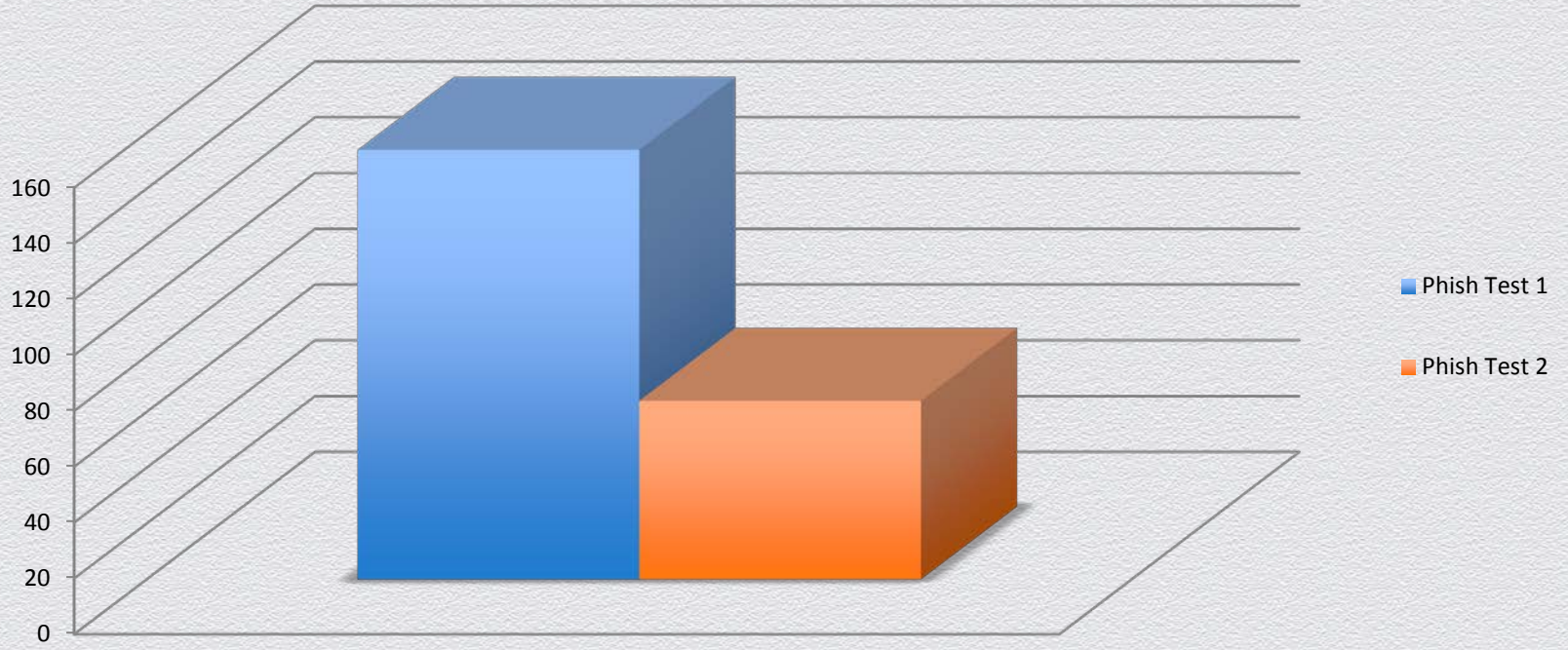
SE Pentest Stage Three: Phishing / Spear Phishing



Goal in this stage:

- Demonstrate a realistic phish
- Educate – tracking
- Employees told at point of click

Phishing Results Series 1 vs Series 2



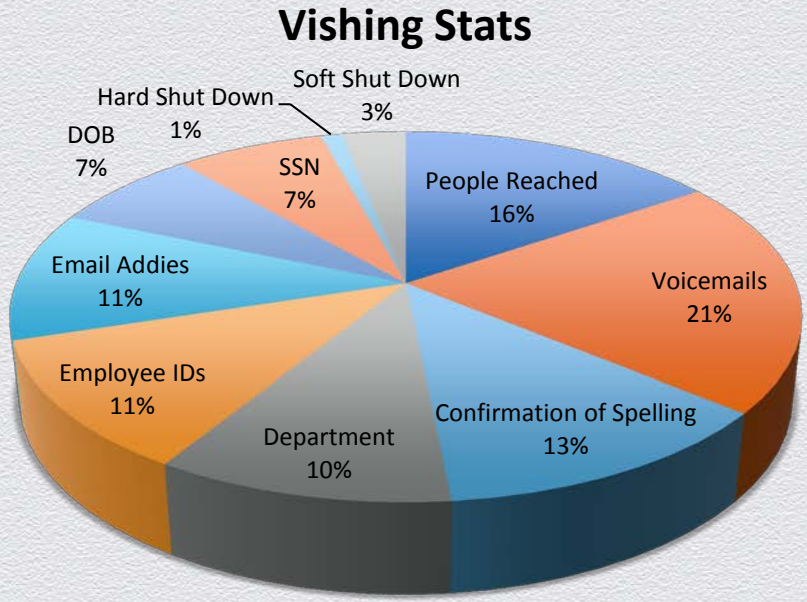
SE Pentest Stage Four: Vishing

Goal in this stage:

- Call as internal employees
- Educate – test protocols of giving out sensitive info
- Lisa from HR or Paul from IT

Name Confirm:	**80%**
Dept Confirm	**67%**
Employee ID:	**73%**
DOB:	**47%**
SSN:	**47%**
Shut Down:	**20%**

Telephone Elicitation - Findings



SE Pentest Stage Five: Onsite Impersonation

Wha

Goal in this stage:

- Test physical access policies
- Access secure areas
- Education – take pictures
- Use pretext that should be identified

We get stopped…

- What can a little bit of information, a cell phone and 15 minutes get us?

Step 3: Critical Thinking

"…the mental process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and evaluating information to reach an answer or conclusion…" - 21st Century Lexicon

Step 3: Critical Thinking

Methodology for developing:

- Proper policies – answer questions employees will have like: What if, What When & How
- Usable scripts – simple processes for the “When” question
- Real world exercises – continual education to create a security minded culture

Conclusion: Summary

Three simple (but not always easy) steps to mitigating SE attacks:

- Be educated
- Get regular check ups
- Create critical thinking infrastructure

And remember, technology won't keep you safe

Question & Answer

Contact Us:

Chris@social-engineer.com

Michele@social-engineer.com