CH53

Confrence on Hacking and Security

Social Engineering
“A hidden threat to network security”

CH53

Confrence on Hacking and Security

Agenda

- Abstract
- Introduction
- Methodology
- Why Social Engineering Works
- Target Attacks
- How to Avoid
- Conclusion

CHASS
Confrence on Hacking and Security

Abstract

- What is the weakest link in Computer Security ?
- The only secure computer is one which is unplugged…
- What is Social Engineering.
  - Collection of techniques used to manipulate people to acquire confidential information

Introduction

- Recipe of Attack
  - An intelligent Brain
  - Great human interaction skills
  - Ability to acquire information from target
  - Using information on appropriate place to gather more information

Methodology

CHASE
Confrence on Hacking and Security

Pretexting

- Creating and using an invented scenario
- Establish acquaintance with target
- Create an image of legitimate person
- Impersonate to one who have authority to know

Pretexting

- Tools for corporate attacks
  - Web sites
  - Marketing agents
  - Client representatives
- Information gathered from above sources can be further used to gain password from middle and low level staff

CH53

Confrence on Hacking and Security

Phishing

- Felonious e-mails
  - Requesting Verification of information
  - Attractive mail subject
- Fraudulent web sites
  - Identical to legitimate web sites
  - URL similar to legal web
- Unclaimed USB and CDs with attractive titles

CH53

Confrence on Hacking and Security

Dumpster Diving

- Valuable information can be found from company dumpster
- Potential Security Leaks
  - Company phone books
  - Company policy manuals
  - Calendars of meeting
  - Events and vacations
  - Login names and passwords
  - Printouts of source code
  - Company letterhead and memo forms
  - Outdated hardware

CH53

Confrence on Hacking and Security

Online social Engineering

- Hackers may obtain information online by
  - Pretending to be network administrator
  - Sending e-mail asking for password
  - Sending pop up windows asking to reenter user name and password to fix some network problem
- Easy network access outlets

CH53

Confrence on Hacking and Security

Impersonation Attack

- Creating some sort of character and playing out role
- The simple role is better.
- Common roles that can be played
  - Repair man
  - IT support
  - Manager
  - President's executive assistant
- A colleague on phone requesting for help
- Flirty and flirtation tone softens the target
- Employee respond in kind especially to women

CH53

Confrence on Hacking and Security

Reverse Social Engineering

- More advanced method of gaining information
- A three step process
  - Sabotage
  - Advertising
  - Assisting

Why Social Engineering Works?

Why social engineering works

- According to psychologists victim's ability to counter argument diminishes under heightened state of emotion.
- Exploiting similarities

  Stranger belonging to your college, university, community or same ancestral town

Target Attacks

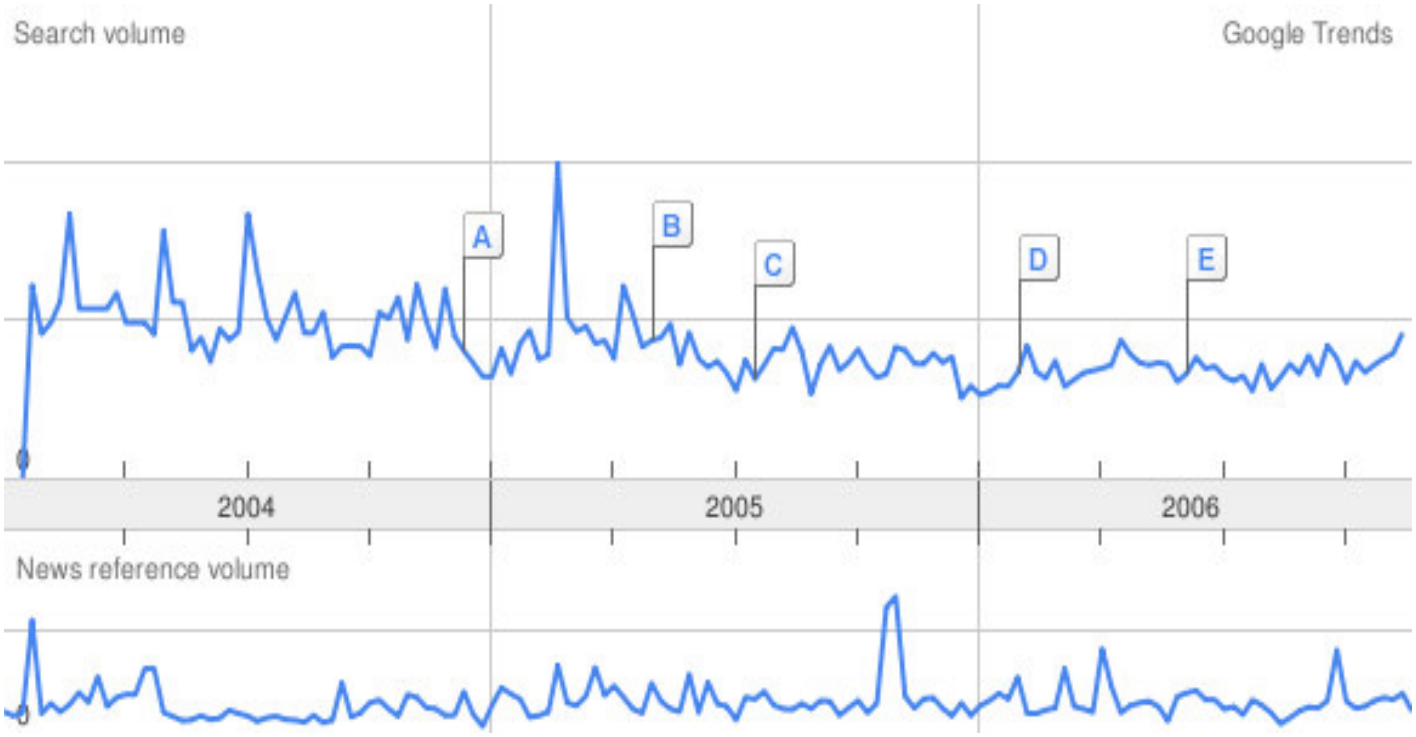
Target Attacks

- Industries that are targeted most by social engineer are those who have above average access control
  - Financial and banking sector
  - Military
  - Government and large IT corporations

Confrence on Hacking and Security

Target Attacks

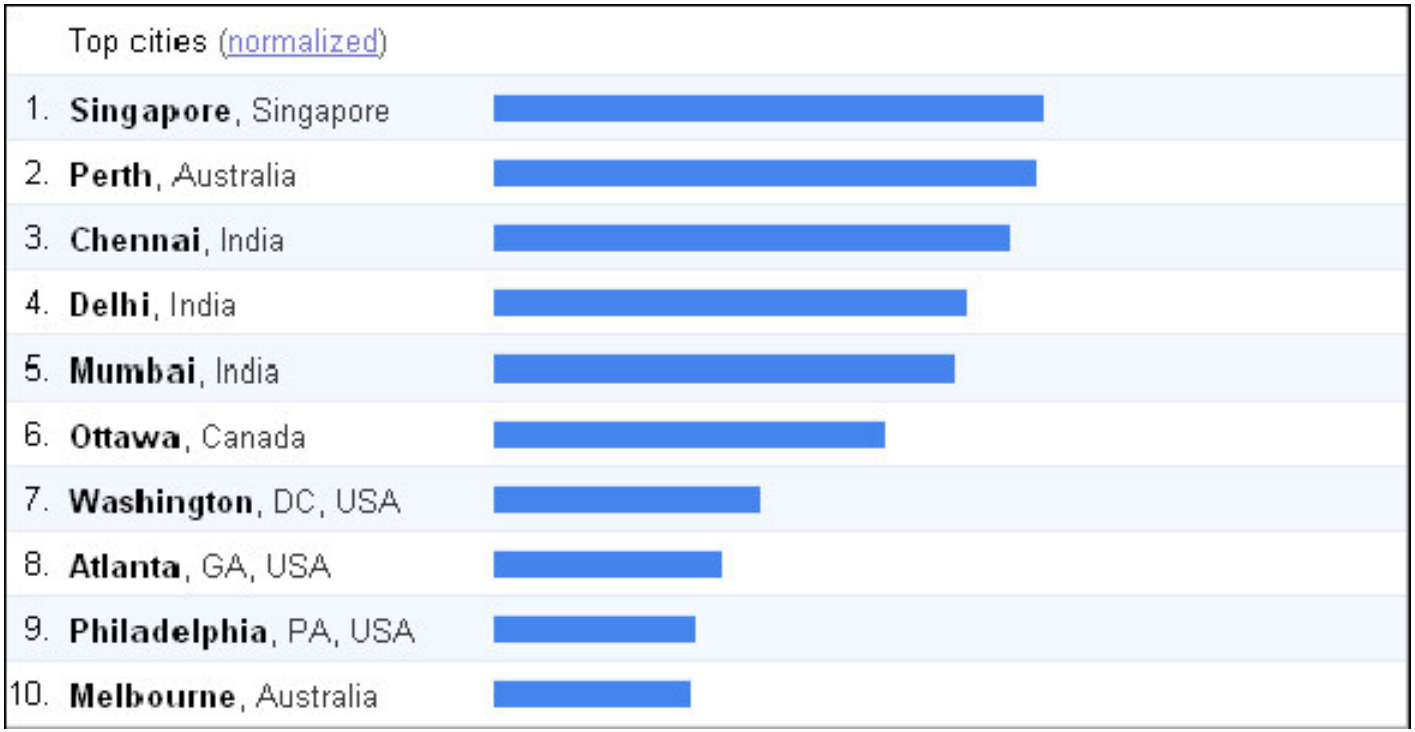
- According to google trends social engineering is a major hack activity during 2004-2006



Confrence on Hacking and Security

Target Attacks

- According to Google Trends major IT cities targeted by social Engineers



How to Avoid Social Engineering Attack

CH53

Confrence on Hacking and Security

How to Avoid…

- Strong information security policy
- Information security training
- Be suspicious of unsolicited e-mail, phone calls or visits.
- Never be afraid to question credentials of strange office workers
- Install and maintain firewalls, anti virus software, anti spyware and e-mail filters

CHASE
Confrence on Hacking and Security

How to Avoid…

- Pay attention to the URL of web site.
- Don’t send sensitive information over internet.
- Don’t reveal personal or financial information in e-mail.
- Don’t provide organization information to anyone.
- Shred any document that is discarded
- Don’t allow employee to download from untrusted websites.

Conclusion

Conclusion

- Getting someone to do something in a way that his logical thinking capabilities are hampered is no easy task. But successful execution of this method are still under-reported as nobody likes to be called a fool or a deceivable dupe

CHASS

Confrence on Hacking and Security

I will be pleased to answer your Queries.