Automating Social Engineering

Alexandru Catalin Cosoi – Head of Online Threats Lab
Daniel Dichiu – NLPT Researcher
Social Engineering

The clever manipulation of the natural human tendency to trust.
Questions that need to be asked

1. What is your name or nickname?
2. What are your interests?
3. Who do you work for?
4. Who are your friends/colleagues?
5. What is your job title?
6. Who is your manager/CEO/director?
7. Who are your family members?
8. Are you married? With whom?
9. Do you have any kids? What are their names?
10. Where do you live? Where were you born?
11. How much do you earn?
12. Where do you stay? How expensive is your house?
Our online identity
Stats

• 24% of Safego users found something malicious posted on their wall
• 90% of malicious Facebook apps were designed to access profile information
• 20% of Android malware discovered so far was designed for phishing or for immediate profit
• 80% of Android malware was designed to extract information from the device
Problem Statement

Get Ready
- Malware that infects computers and steals data or becomes part of a botnet
- Spam messages that contain infected attachments
- Fake shops and scams which provide the necessary investment for the underground economy

Get Set
- Find people and identify their online identity
- Spread spyware that will constantly monitor their activity

Go
- Create unique messages based on the victim’s social profile
- Convince them to disable the protection if necessary
Steps of a Targeted Attack

email address
- Social media accounts
- Complete Name and Nicknames

LinkedIn & Social Networks
- Gender
- Workplace related info
- List of friends and coworkers
- Field of activity and interests

Aggregate data into complete social profiles
- Use search engines to complement the information extracted from SNS
- Use NLP techniques to parse and use data
Google search

Alexandru Catalin Cosoi - Romania | LinkedIn
ro.linkedin.com/in/catalincosoi - Cached
Romania - Head of Online Threats Lab at BitDefender - BitDefender
View Alexandru Catalin Cosoi's (Romania) professional profile on LinkedIn. LinkedIn is the world's largest business network, helping professionals like ...

Catalin Cosoi | Facebook
www.facebook.com/catalin.cosoi - Cached
Catalin Cosoi is on Facebook. Join Facebook to connect with Catalin Cosoi and others you may know. Facebook gives people the power to share and makes ...

MalwareCity : Authors - Catalin Cosoi
www.malwarecity.com/authors/catalin-cosoi.html - Cached
Catalin Cosoi - Security researcher by day, developer by night and stand-up comedian wannabe, Alexandru Catalin Cosoi spends almost the entire day in front ...

Catalin Cosoi - BitDefender
www.bitdefender.com/blog/author/Catalin-Cosoi.html - Cached
BitDefender security blog. Read daily our antivirus blog posts. Stay up to date with what's happening in the security world.

Articles by Catalin Cosoi | Network Security Edge
www.networksecurityedge.com/author/104 - Cached
21 Dec 2009 – Cyber Threats | Guest Opinion | Catalin Cosoi Wednesday, February 17, 2010. Whenever we enter a new decade, many of us like to take stock ...

Catalin Cosoi - Google+
123people search

People search results for: Catalin Cosoi

Related Pictures (19)

Email Addresses (3)

acosoi@bitdefender.com
www.catalincosoi.com

me@catalincosoi.com
www.catalincosoi.com

carmen.cosoi@nielsen.com
projects.csail.mit.edu
123people search
## Pippl Search

**Catalin Cosoi, Romania**

### Professional & Business
- **Alexandru Catalin Cosoi**, Head of Online Threats Lab at BitDefender, Romania...  
  - Professional Profile & Networking - LinkedIn
- **Catalin Cosoi**, RO, private, Security and Investigations...  
  - Professional Profile & Networking - LinkedIn

### Publications
- Systems and methods for generating signatures for electronic communication...  
  - Patent - US Patent & Trademark Office

### Results for Catalin Cosoi without Romania

#### Personal Profiles
- **Catalin Cosoi**  
  - Personal Web Profile - Facebook
- **Catalin Cosoi, Male, 28...**  
  - Personal Profile - Bebo

### Sponsored Tip: Find hidden profiles and photos across MySpace, Facebook and 40+ networks...

#### Photos
- Photo & Video Sharing - Photobucket
- Photo & Video Sharing - Photobucket

#### Videos
- BitDefender Q3 Top Five E-Threats, 3 min - Sep 29, 2010 - Uploaded by...
- BitDefender Tips to Stay Safe from Q3 E-Threats, 1 min - Sep 29, 2010 - Uploaded by...
- Social media threats and targeted attacks, 7 min - Mar 29, 2011 - Uploaded by...
Example 1 - background

Choose VIC
- Full Name
- Location
- Gender

Classical Nigerian Scam
Dear Alexandru Cosoi,

I'm writing to you in a time of sadness and desperation. I'm not sure if you know this, but two decades ago, your cousin, [insert random Romanian name] Cosoi moved to Nigeria. Here he managed to start a shipment business which in time managed to become quite successful. He has two sons [another random Romanian name here] Cosoi and [yet another random Romanian name here] Cosoi, which moved to UK. Your cousin is dying, bla bla bla, so we need to transfer money out of Nigeria to UK, in order to provide a decent living for his kids.

We ask for your help because you are family and we wouldn't bother you if it weren't important, and also, it would be better to keep this between us.
Example 2 - background

Choose VIC
- Company name
- Job Title
- Avoid if Job is related to tech dep

Find HR Manager
- eMail address
- Full name

Attack
- eMail containing a PDF file with new job openings
- Preferably VIC must not be a senior
Example 2 - context

Dear [full name]

Since we’ve been very pleased with your activity so far, I would like to take this opportunity to thank you for your dedication and involvement.

As the HR team is starting a new project of personal development to boost our employees’ career plans, please find attached the PDF file containing what we believe to be a successful career plan for you in this company.

HR Director
Example 3 - background

Choose VIC
• Company Name
• Job Title
• Avoid tech users

Create Credibility
• Find another employee
• Similar job
• Preferably working together

Pick a topic
• Find someone with a higher position in the organization
• Related job title (preferably their manager)
Example 3 - context

Dude!!! (also knowing the gender helps)

Have you seen the news?!  
http://www.getInfected.com

Is it just me, or [manager name] is leaving us?  
I’m very very upset that we have to find out about this from the media and not directly from him/her.

Grrrr!!!
Experiment

- 1996 randomly selected email addresses
- 100 registered a LinkedIn account (5%)
- 370 registered a Facebook account (18.5%)
- 70 registered a Pulse account (3.5%)
- Nickname or Real Name found for 540 individuals
- A valid photo was found for 427 individuals (21%)
- Gender was found for 540 users and determined for an additional 178
Wrapping up

1. Social engineering works.
2. Social engineering can be automated.
3. The better your identity is represented online, the higher the chances of becoming a victim.
4. We need to understand the addiction to social networks and the fact that users will post information about themselves online, ignoring the consequences.
5. Education can work. It’s our duty to educate both users and employees about social engineering and how their own data can turn against them.