UNSW SYDNEY | Australia's Global University

Engineering

Taste of Research Summer Scholarship Program

Social Network as a Vector for Malware

Author: Sijun Zhu

Supervisor: Prof. Salil Kanhere, Arash Shaghaghi

Research theme: The Digital Future

SPIEGEL ONLINE — GCHQ Used **Fake LinkedIn Pages** to Target Engineers

CNN politics — Report: Iran-based hackers **spy using fake LinkedIn profiles**

Background & Motivation

Social Networks are Attractive Targets for Hackers

- **3.03 billion** users, about **80%** of Internet users.
- **18** victims of cybercrime per second, **556 million** victims per year.
- Global Cyber-security market size **doubled** to **127 billion** in 2017 vs. 2011.

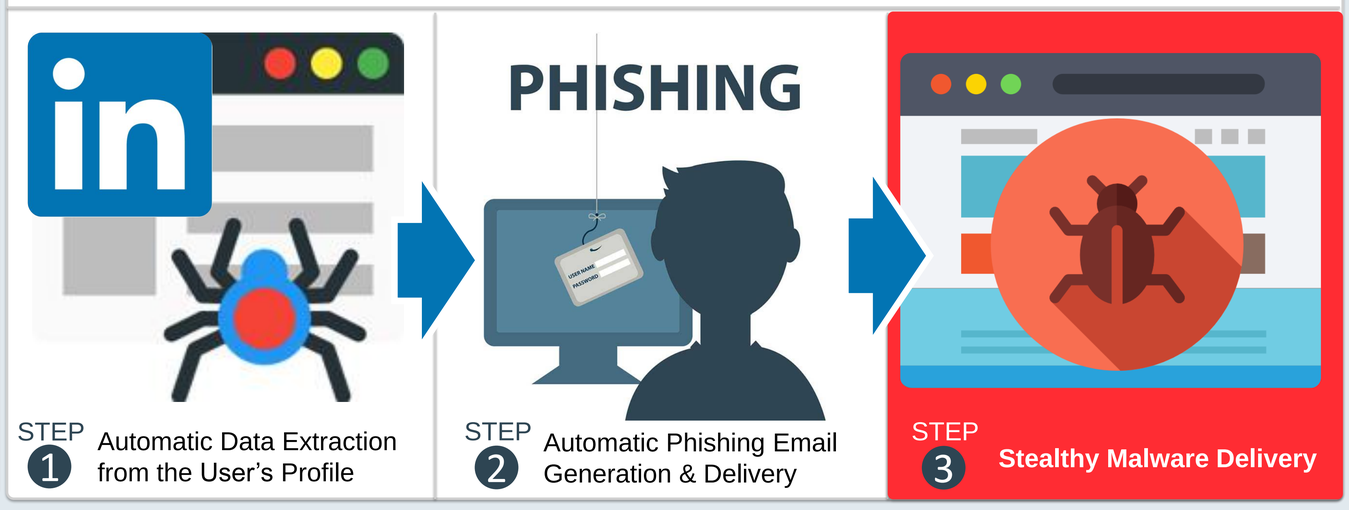
Why LinkedIn?

- Ranked **6th** among social networks in Australia, and **14th** globally.
- Large sum of personal information shared publicly - for recruiters, reputation, personal marketing, etc.

Scope & Aims

- Understand how social networks are used to deliver malware & study how users and providers can prevent them - focused on Australian users.
- Replicate malware delivery attacks through LinkedIn.
- Identify underlying technical challenges.
- LinkedIn security analysis - focused on user-side.
- Investigate protection requirements.

Attack flow



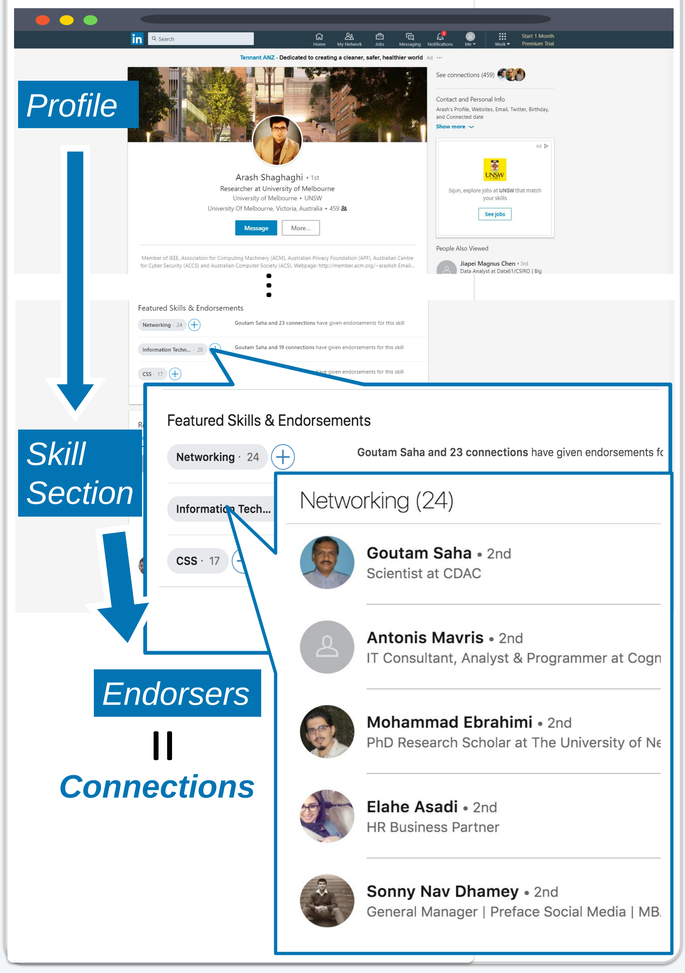
Vulnerabilities Discovered

LinkedIn profile - Skills section:

- Only connections of the target can endorse his skill.
- Skill section is visible to public.
- Skill section leaks target's connection status, which is used in our attack.

Unencrypted link to JSON file

- Open to public and allows crawlers to automatically extract information.

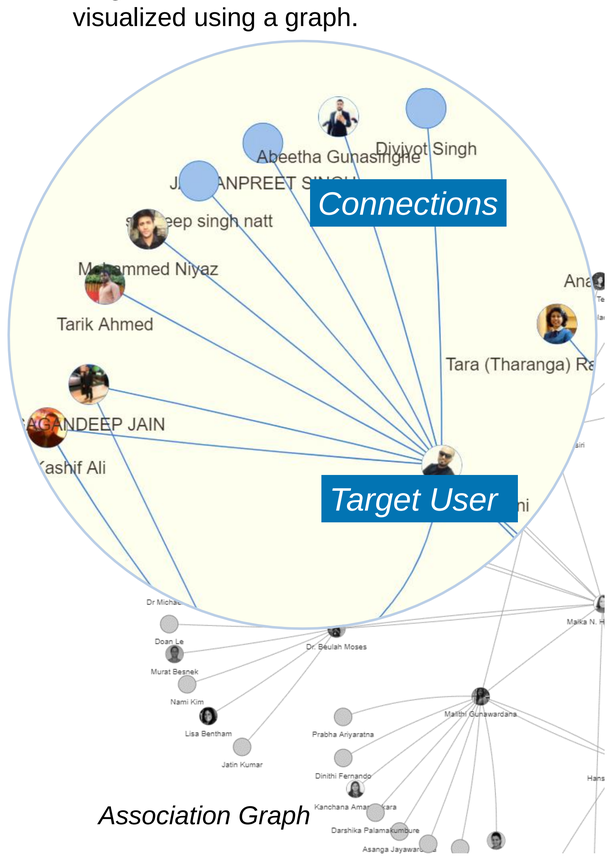


Attack Implementation

STEP 1 *Automatic Data Extraction from the User's Profile*

- Python Web Crawler extracts skill section data in JSON file.
- URL of JSON file is easy to find (it has a fixed format in relation to the user's profile ID).

Target's connections can then be visualized using a graph.

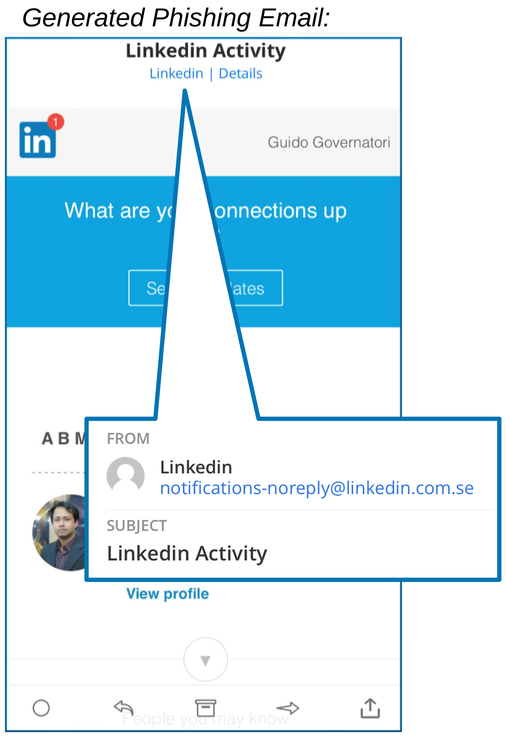


Association Graph

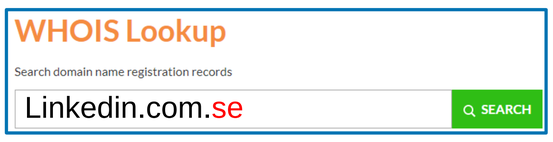
STEP 2 *Automatic Phishing Email Generation & Delivery*

- Generate Phishing email from extracted information – look exactly like the ones LinkedIn sends.
- Links in email direct user to Phishing webpage.

Generated Phishing Email:



Who owns "linkedin.com.se"?



STEP 3 *Stealthy Malware Delivery*

- Hundreds of vulnerabilities are discovered for platforms each year – see cvedetails.com
- On-going investigation to use Spectre (Zero-Day vulnerability reported in 2017).
- Simulated few attacks to gain full unrestricted access through existing vulnerabilities. Example:

Simulation Environment	
Attacker's OS	Kali Linux 2018.1
Framework	Metasploit 4.16.17
Target OS	Windows 7
Target Browser	IE8, Firefox
Vulnerability Tested	CVE-2015-0335 (Flash)

Recommended Solutions

For LinkedIn

- Encrypt the URL to the JSON file to weaken the its relationship with user's profile ID.
- Use stricter anti-crawler policy.
- Purchase similar international domains and subdomains.
- Verify legitimate users through mobile phones, valid organizational emails, etc.

For Users

- Increased user awareness & training: Australian users tend to share more than the others!

Contributions

- ✓ Two main LinkedIn vulnerabilities that leak user data.
- ✓ Crawler that exploits the vulnerabilities to build Association Graphs.
- ✓ Registered LinkedIn.com.se to bypass SPAM filters for Phishing attack.
- ✓ Report and crawler available online.
- Report/news about the issue to increase user awareness.
- Set of recommendation for Australian users to protect themselves on LinkedIn.
- Bug report to LinkedIn.
- Academic paper about the vulnerability & attack.

Future Work

- Investigate attack success rate under controlled settings.
- Incorporate Machine Learning into the crawler (Deep Learning).
- Finish implementing the attack through Spectre vulnerability.