



Using Online Activity as Digital Fingerprints to Create a Better Spear Phisher

Joaquim Espinhara & Ulisses Albuquerque
JEspinhara@trustwave.com UAlbuquerque@trustwave.com



Agenda

- Introduction
- Motivation
- Background
- HowStuffWorks
 - Our Approach
- μphisher
- Demo
- Future Work
- Conclusion

About us

- Joaquim Espinhara
 - From Aracaju, Brazil
 - Security Consultant at Trustwave Spiderlabs
- Ulisses Albuquerque
 - Coder for offense & defense... as long as it's fun!
 - Lab Manager at Trustwave Spiderlabs





INTRODUCTION





OUR MOTIVATION



Our Motivation

- Why?
- Tools available



BACKGROUND

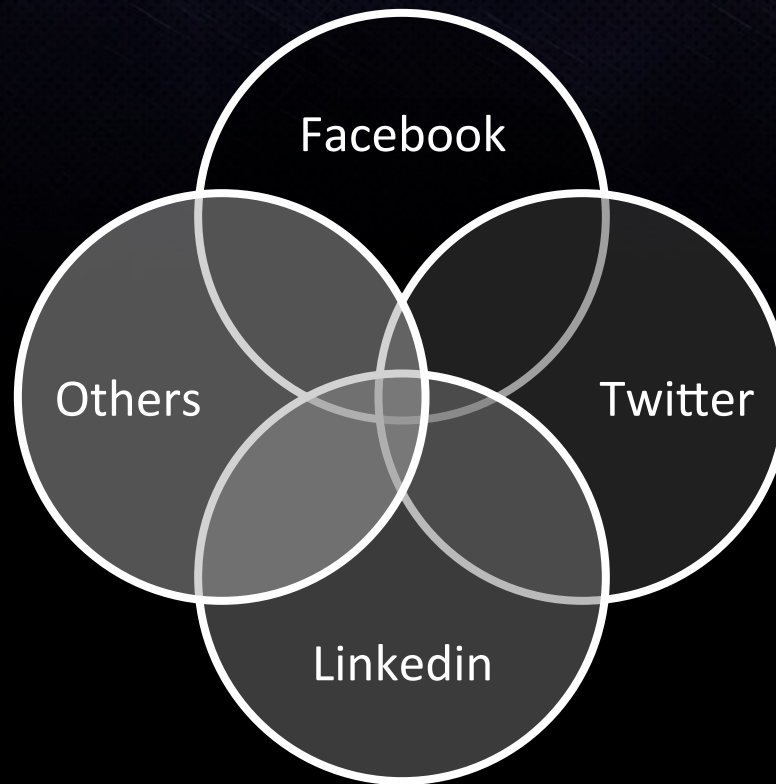


Background

- Social Networks
- Social Engineering
- Data Mining
- Natural Language Processing - NLP

Background

- Social Networks



Background

- Social Networks
 - Communication channel for keeping in touch with someone (Facebook, Twitter)
 - Media sharing (Instagram)
 - Specialized networks (GetGlue, Triplt, LastFM)

Background

- Social Engineering
 - Phishing



<http://www.d00med.net/uploads/0d832c77559a2070a766f899e7efb783.png>

Background

- Data Mining
 - What is it?
 - What do you need know about it?
 - How do we use it?

Background

- Data Mining



"Had lunch with
@urma and
@jespinhara today
#tgif #lunch"

Data cleaning

"Had lunch with
@urma and
@jespinhara
today"

Data integration

"Had lunch with
@urma and
@jespinhara
today"

Data
normalization

"Had lunch with
@urma and
@jespinhara today
(2013-06-05)"

Background

- Natural Language Processing – NLP
 - What is it?
 - What do you need know about it?
 - How do we use it?
 - Text analysis



HOWSTUFFWORKS



Our Approach

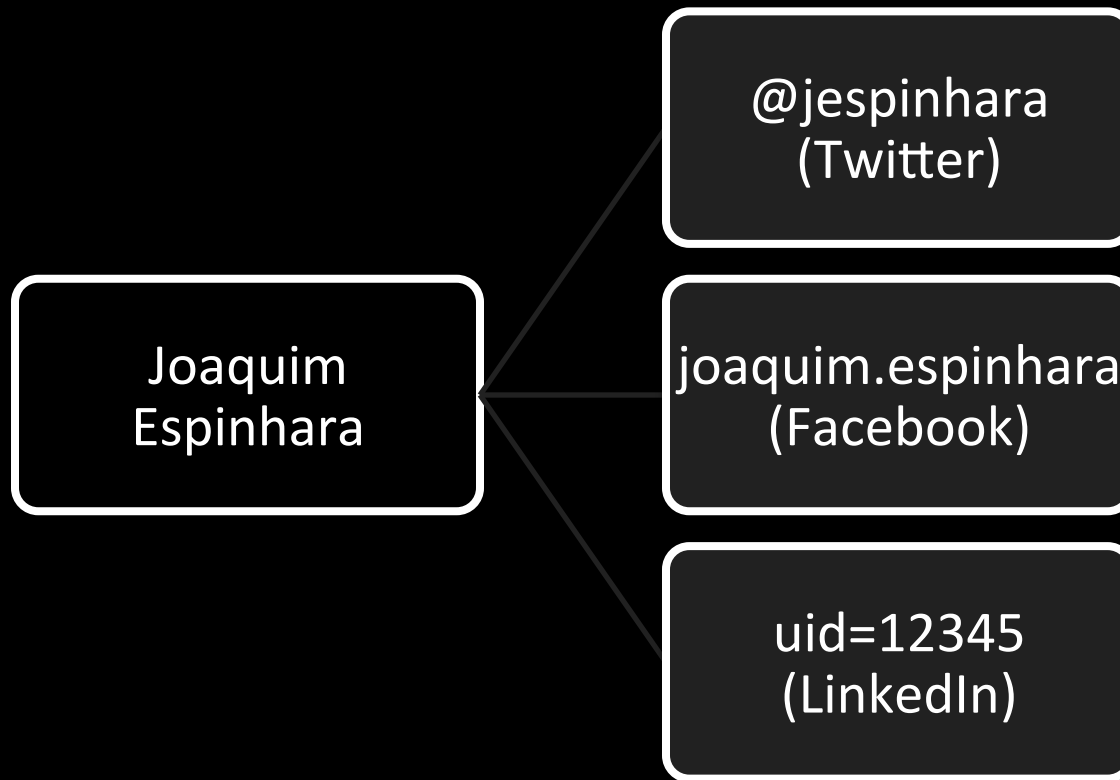
Identifying
the subject to
profile

Collecting
social
network data

Analyzing and
building the
profile

Our Approach

- The Unknown Subject (*Unsub*)

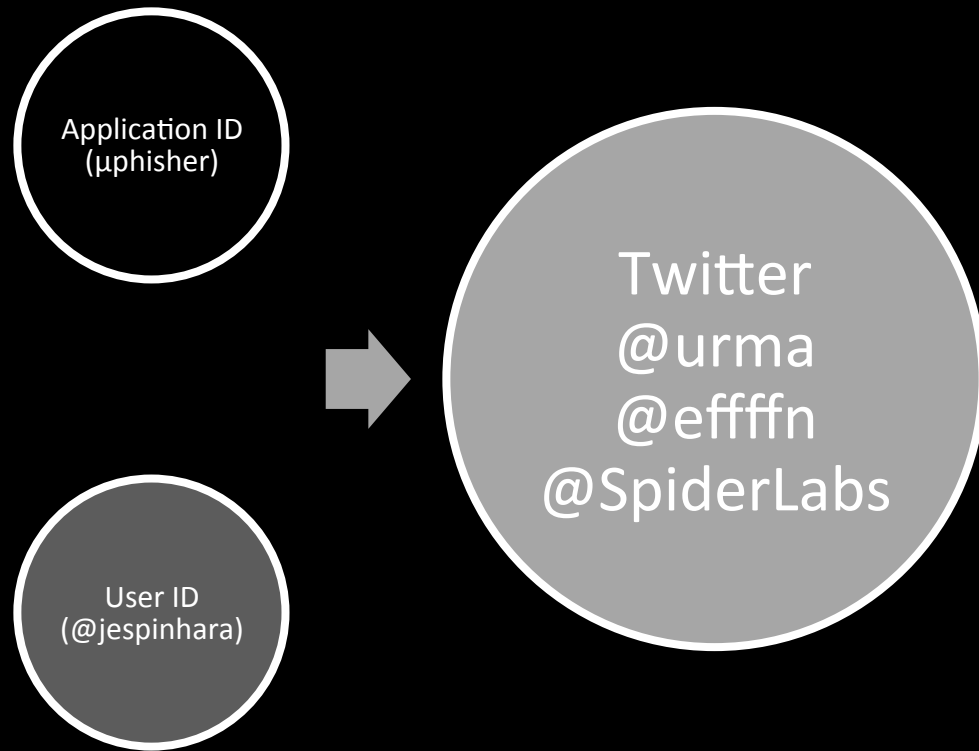


Our Approach

- Data Collection
 - Social Network IDs
 - Official APIs
 - Web Scraping
 - OAuth

Our Approach

- Data Collection - Twitter





μPHISHER



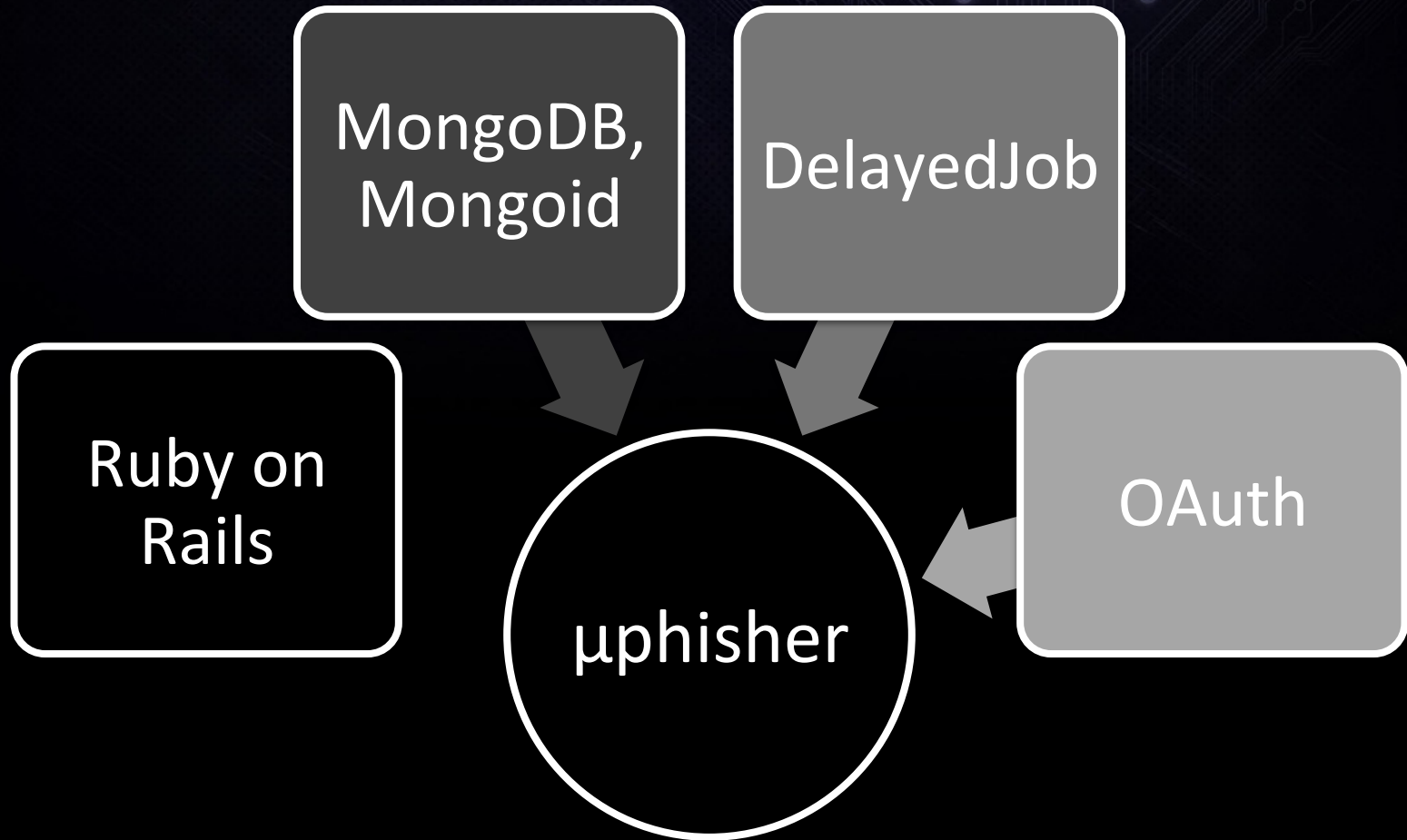
μphisher

- Reference implementation
- Goals
 - Validate potential *unsub* content
 - Assisted textual content input

μphisher

- Web Application
- Twitter only (for now)
- Open Source (GPLv3)

μphisher



μphisher



μphisher

The screenshot shows a web browser window with the following elements:

- Browser Tab:** μphisher
- Address Bar:** localhost:9292/index.html
- Navigation Menu:** μphisher | Home | Unsubs | Data Collection
- Header:** μphisher automated social engineering profiling
- Controls:** Six sliders for Word Frequency, Sentence Length, Sentence Count, Phrase Count, User References, and Pronoun Usage. An Overall Score slider is also present.
- Text Area:** Code hackaton with @jespinhara for the latest μphisher rele
- Buttons:** release, relet



DEMO (FINGERS CROSSED)





DOWNLOAD

[HTTPS://GITHUB.COM/URMA/MICROPHISHER](https://github.com/urma/microphisher)



Future Work

- Support for additional data sources
- Machine learning
- More metrics and feedback for assisted input



CONCLUSION





THANK YOU!

