Stanford University | CS 114 Guest Lecture | April 11, 2022

Studying Malicious Online Activity:

A Data-driven Approach

Dr. Jeremiah Onaolapo

University of Vermont

A Brief Bio

- **Affil.:** Assistant Professor of CS, University of Vermont
- **Was:** Postdoc, Northeastern University, Boston
- **Was:** CS PhD Student, University College London (UCL)

Background

- Malicious actors keep evolving
- Stakeholders have to be current
  (incl. researchers and the general public)
- To **disrupt** malicious activity, first understand it

Approach

- Build systems to answer pertinent research questions
  Data-driven approach

- Leverage crawlers, NLP, ML, *etc.*

- Interdisciplinary nature
  Computer Science + Criminology + Sociology + more

SocialHEISTing Backstory

- Studied the behavior of cybercriminals
- By designing, building, and deploying honeypots
- And applying other research methods, too
- Ethics is always a serious concern!

Gmail Honeypot: Prior Work

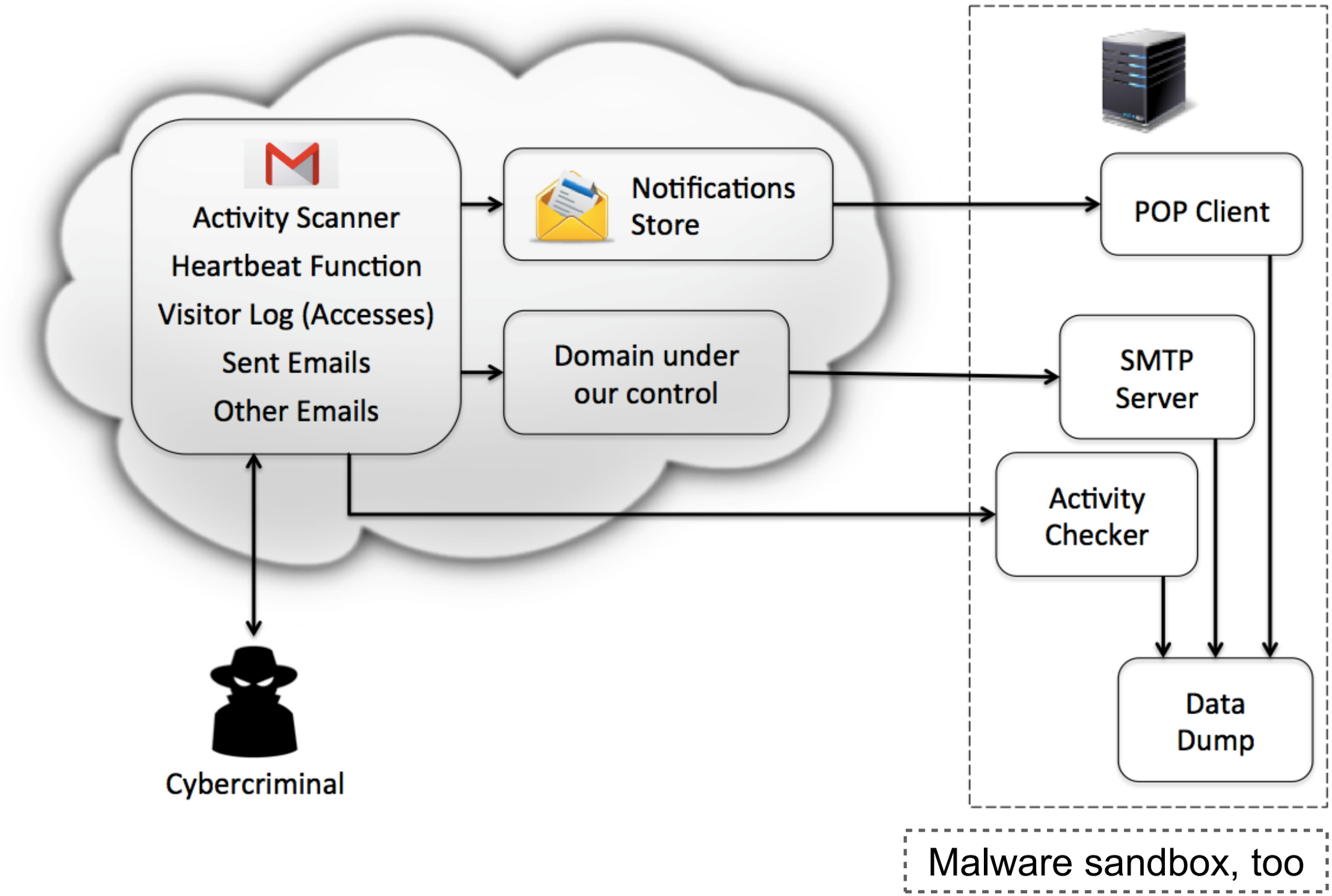
- Malicious activity in webmail accounts (Bursztein et al. 2014)
- Difficult to study unless in charge of large online service
- Until recently...

Bursztein et al. 2014. Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild. In *ACM Internet Measurement Conference (IMC)*, 2014.

Gmail Honeypot: Goal + How

- Study actions and access patterns of cybercriminals in compromised online accounts
- Minimize the risk of harm to humans
- Publicly available at https://github.com/jonaolapo/gmail-honeypot

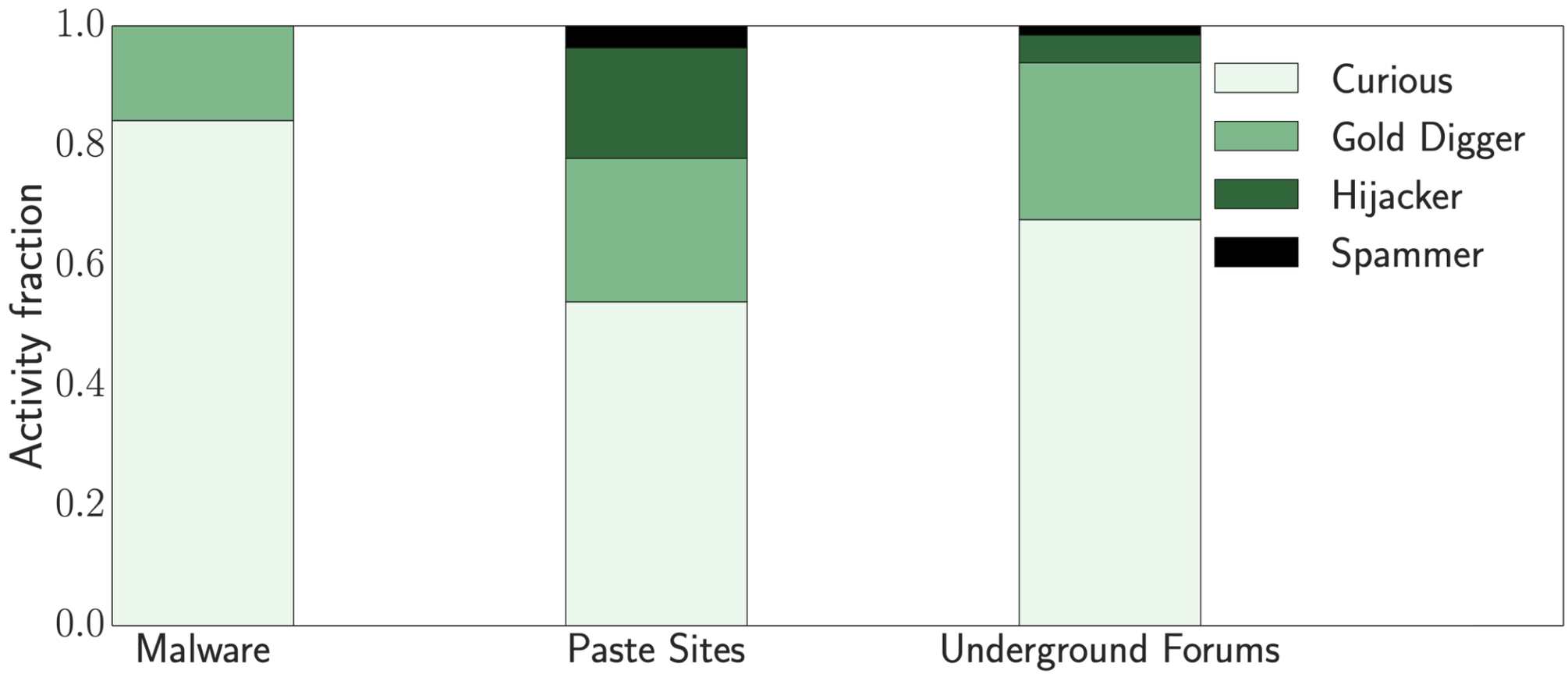
Gmail Honeypot



Gmail Honeypot: Activity

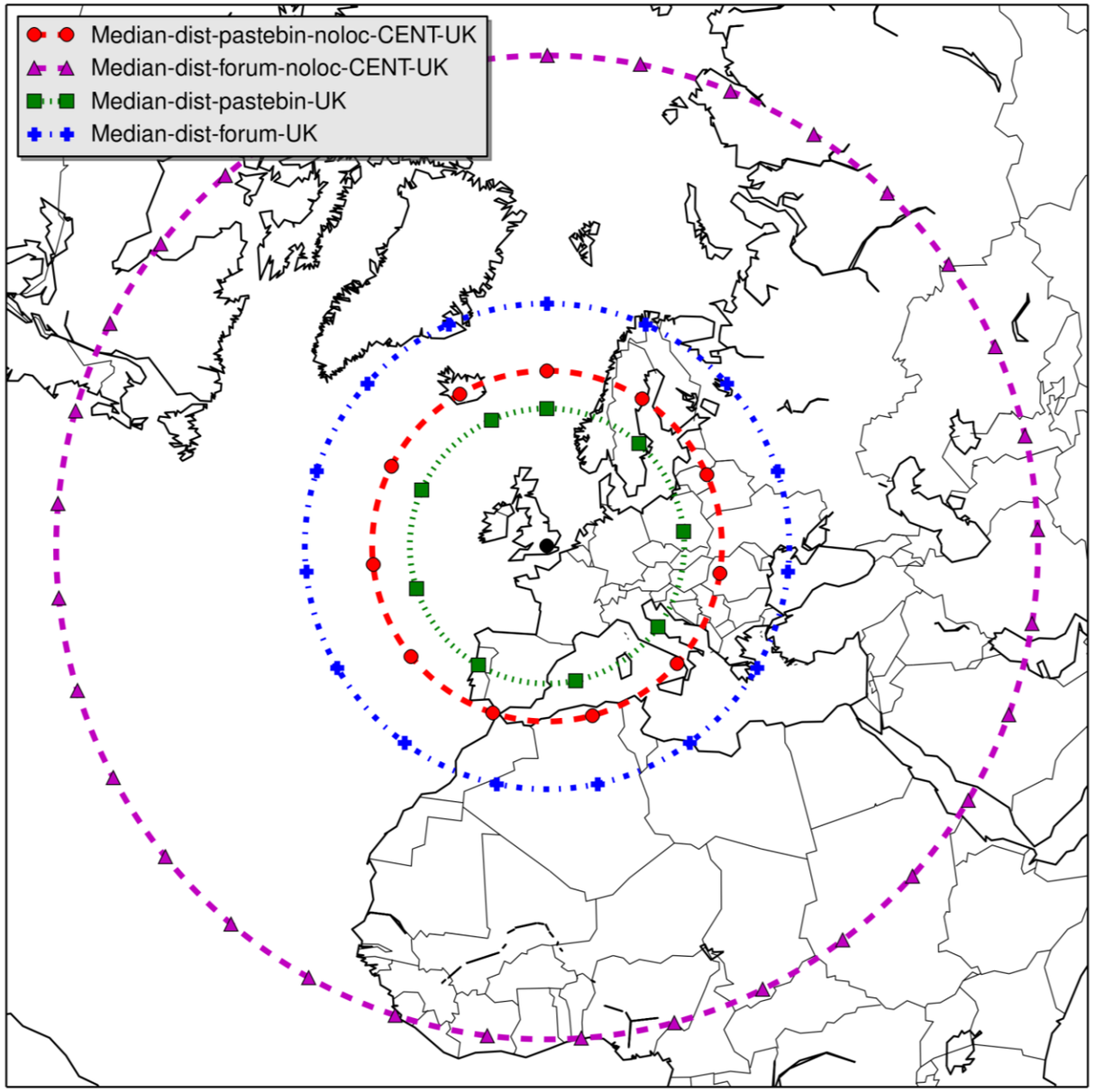
- 100 Gmail accounts populated using the Enron corpus
- Leaked via paste sites + forums + malware
- Monitored for 7 months
- 327 unique accesses from 29 countries

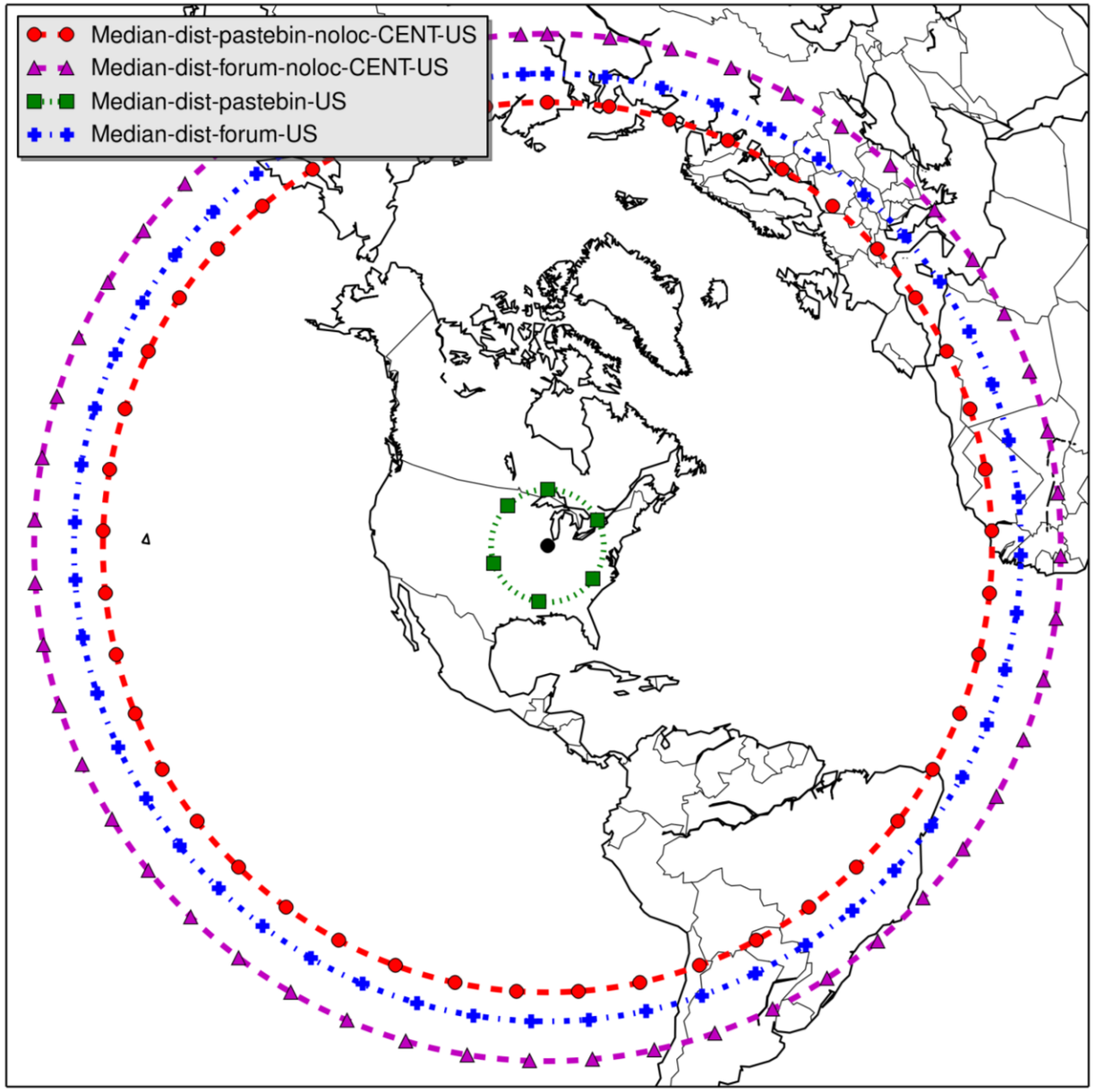
Gmail Honeypot: Activity



A second round of malware accesses showed up weeks after first round.
Supports research on credential theft via malware (first stockpile, then sell).

Gmail Honeypot: Location Tricks





Paste outlet: CvM tests revealed statistical significance.

What Happens After You Are Pwnd: Understanding the Use of Leaked Webmail Credentials in the Wild

Jeremiah Onaolapo, Enrico Mariconti, and Gianluca Stringhini
University College London
{j.onaolapo, e.mariconti, g.stringhini}@cs.ucl.ac.uk

ABSTRACT

Cybercriminals steal access credentials to webmail accounts and then misuse them for their own profit, release them publicly, or sell them on the underground

Keywords

Cybercrime, Webmail, Underground Economy, Malware

1. INTRODUCTION

Available at https://www.uvm.edu/~jonaolap/papers/imc16gmail.pdf

Presented at ACM IMC 2016

Finalist at CSAW Europe 2017


BBC

Home News Sport More

NEWS

Home | Prince Philip | Coronavirus | Video | World |

US & Canada | UK | Business | Tech | Science | Stories

Tech

How hackers handle stolen login data

By Mark Ward
Technology correspondent, BBC News

17 October 2016

Available at https://www.bbc.com/news/technology-37510501

Press coverage

See Also

The Cause of All Evils: Assessing Causality Between User Actions and Malware Activity

Enrico Mariconti, Jeremiah Onaolapo, Gordon Ross, and Gianluca Stringhini

University College London
{e.mariconti,j.onaolapo,g.stringhini}@cs.ucl.ac.uk,g.ross@ucl.ac.uk

Presented at USENIX CSET 2017

See Also

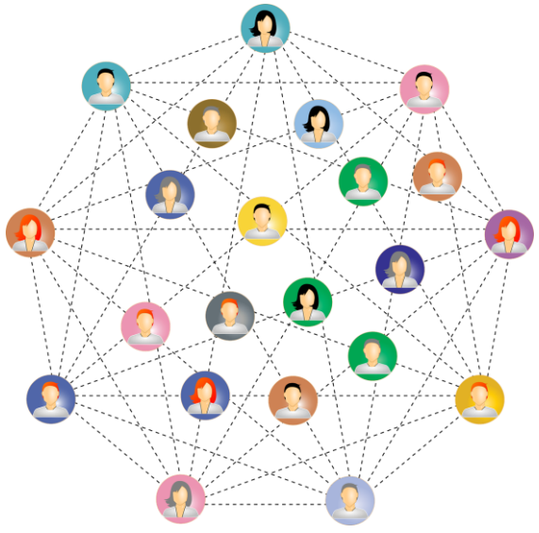
BABELTOWER: How Language Affects Criminal Activity in Stolen Webmail Accounts

Emeric Bernard-Jones, Jeremiah Onaolapo, and Gianluca Stringhini
University College London
emeric.bernard-jones.15@ucl.ac.uk
{j.onaolapo,g.stringhini}@cs.ucl.ac.uk

Presented at TheWebConf CyberSafety Workshop 2018

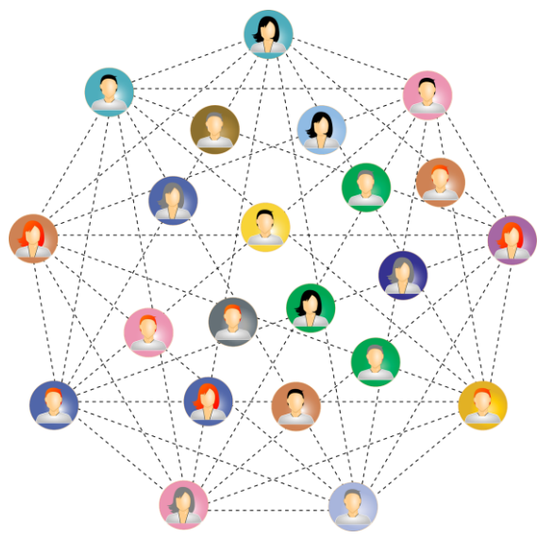
Later: Social Accounts

- Collaboration with Facebook contacts established via my advisor in grad school, Dr. Gianluca Stringhini
- Meetings in London office
- NB: Facebook is now known as Meta



Background

- Social accounts present/reveal demographic attributes
  (age, gender, location, and occupation, etc.)
- Interesting contents in social accounts!
- Accumulate personal info + sentimental value over time
- Attributes can be abused by malicious parties



Goal

- To understand the effects of demographic attributes on attacker behavior in stolen social accounts
- Without harming any real users

Create + populate honey accounts

Configure monitor infrastructure

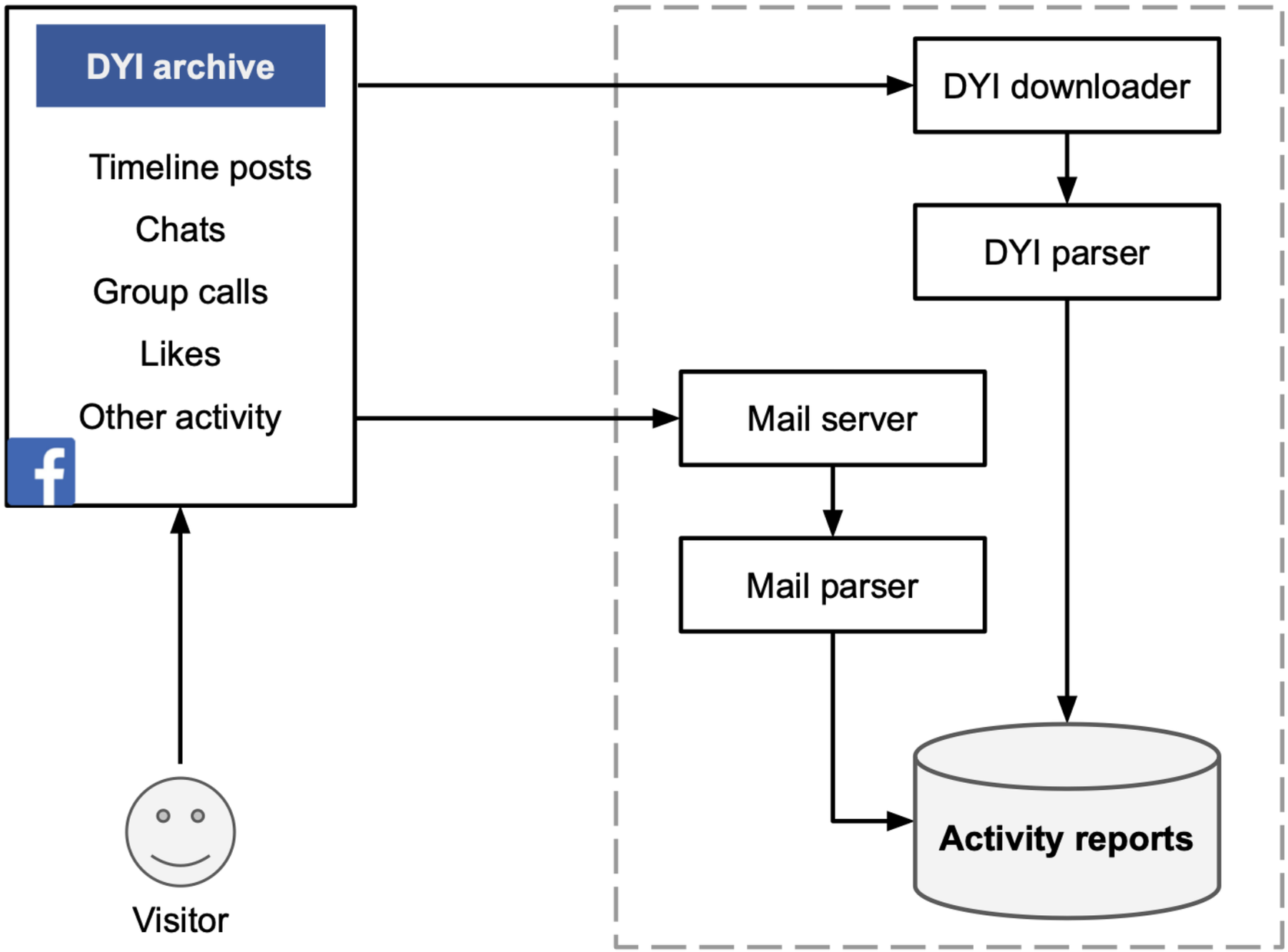
Leak honey credentials

Record + analyze data

Better understand cybercriminal behavior

Pipeline

Data Collection System



Ethics

- Used test accounts; isolated from regular FB social graph
- Used publicly available stock photos and social posts
- Facebook contacts kept an eye on the accounts
- Obtained ethics approval from university

Experimental Setup

- 1008 realistic Facebook accounts
- Populated with publicly available data (sanitized)
- Leaked credentials to two-thirds of the accounts
- Via paste sites on Surface Web + Dark Web
- Monitored accounts for 6 months

Actions

- 322 unique accesses to
- 284 accounts, resulting in
- 1,159 actions
- *Curious*, *searcher*, and *chatty* activity dominates the actions table

Age of Account

Criminals...

- **Add/remove friends:** adult accounts > teen accounts
- **Edit profiles:** adult accounts < teen accounts
- **Create posts, chat:** adult accounts < teen accounts

Gender of Account

Criminals...

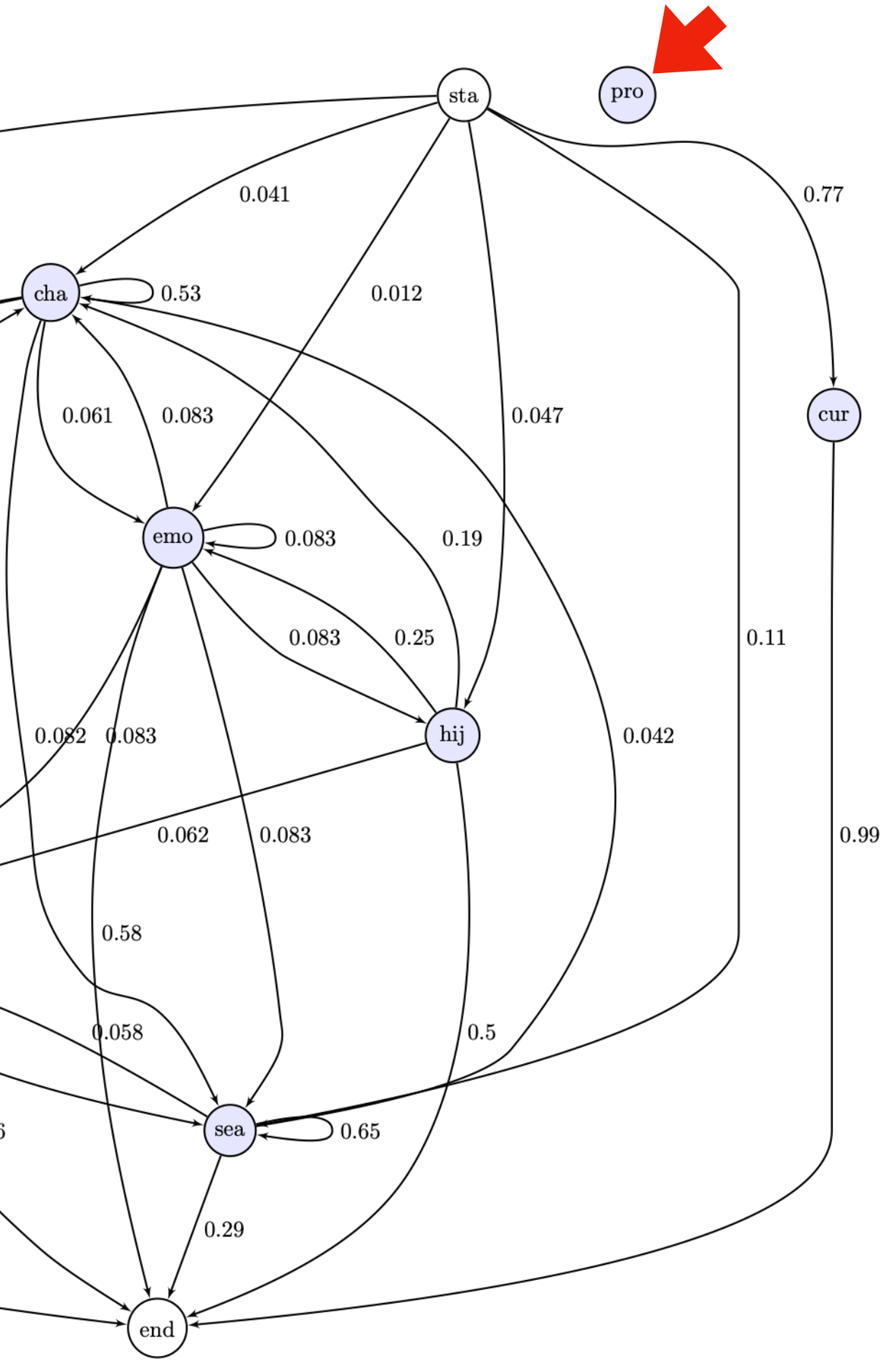
- **Add/remove friends:** female accounts > male accounts
- **Edit profiles:** female accounts (none) < male accounts
- **Search:** female accounts < male accounts

Action Sequences

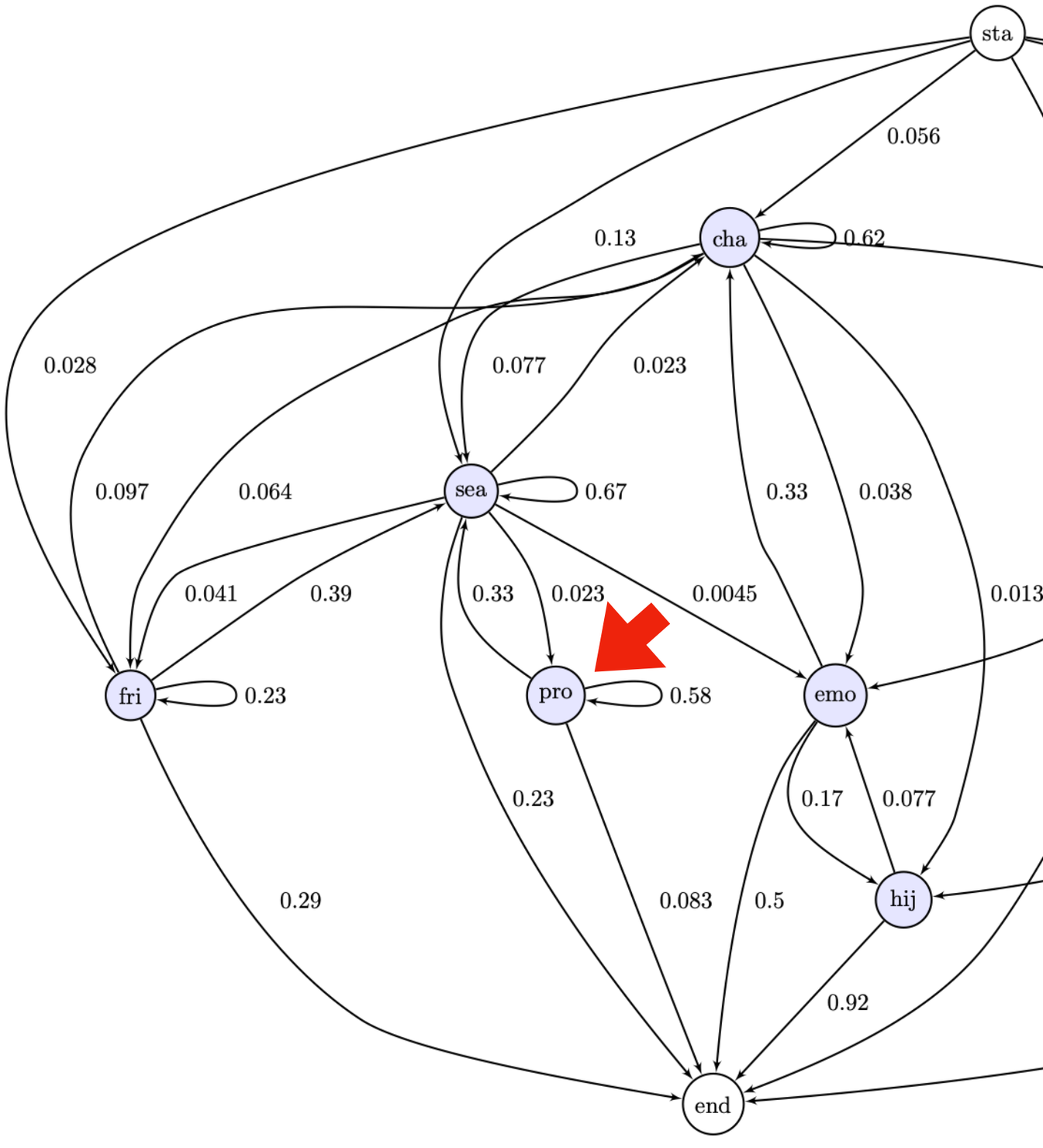
- Modeled action sequences as graphs; edge weights as probabilities of transitions

- Transitions from *action* to *other action* differed across the age and gender dimensions of victim accounts

- Illustrative example: *emo* → *cha* → *hij*



Female accounts



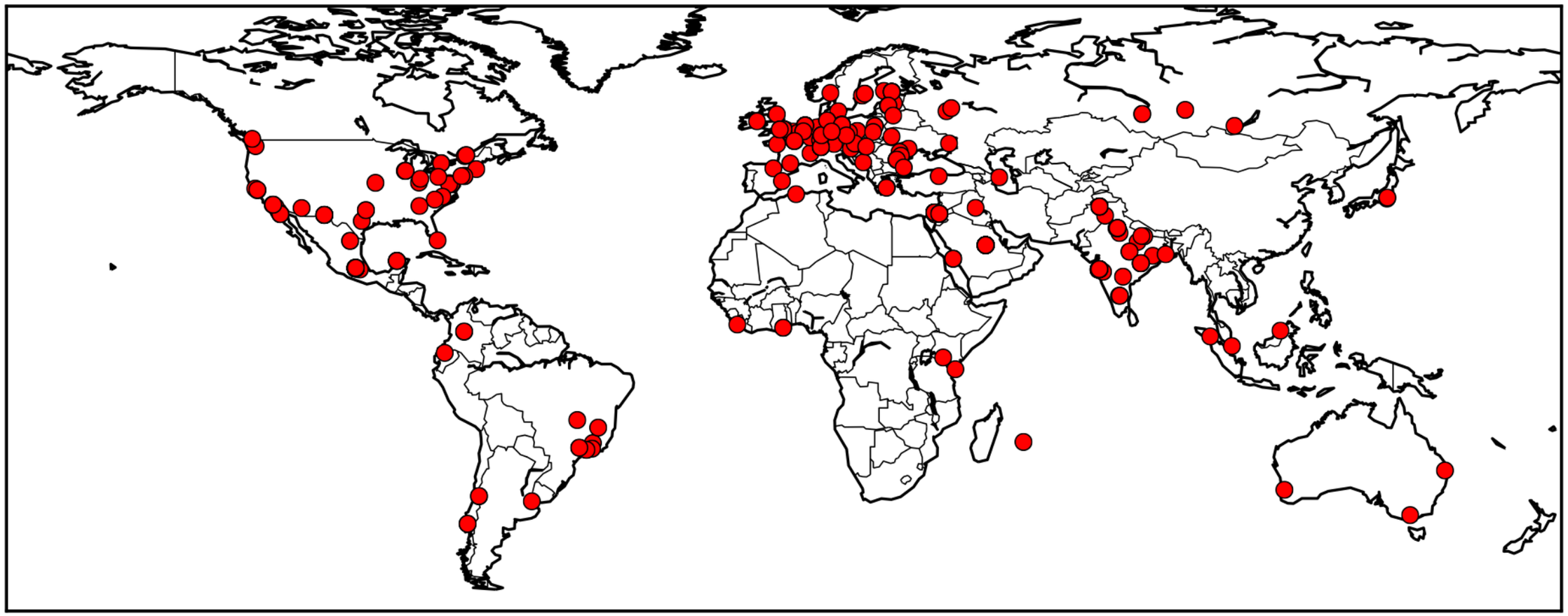
Male accounts

Origins of Accesses

- 415 IP addresses (a mix of IPv4 and IPv6)
- 53 countries
- 39 TOR exit nodes

Some may be VPNs and proxies

Origins of Accesses



SocialHEISTing:
Understanding Stolen Facebook Accounts

Jeremiah Onaolapo
University of Vermont
jeremiah.onaolapo@uvm.edu

Nektarios Leontiadis
Facebook
leontiadis@fb.com

Despoina Magka
Facebook
despoinam@fb.com

Gianluca Stringhini
Boston University
gian@bu.edu

Available at https://www.uvm.edu/~jonaolap/papers/usenix2021socialheisting.pdf

Won a $92K Secure-the-Internet grant (many thanks to Facebook)

Presented at the 2021 USENIX Security Symposium

Hackers act differently if accessing male or female Facebook profiles

TECHNOLOGY 10 March 2021

By Chris Stokel-Walker

Available at https://www.newscientist.com/article/2270552-hackers-act-differently-if-accessing-male-or-female-facebook-profiles/

Press coverage

Doing Research

- Let us explore the *behind-the-scenes* backdrop to the *behind-the-scenes* buildup to the SocialHEISTing paper

First

Keep things simple!

On Research

- Excerpted from an invited blog I wrote once upon a time…

- Available at https://www.hetcnn.nl/nieuwsitems/het-cnn-blog-reeks-ervaringen-met-criminologische-phd-trajecten-deel-3/

- NB: The main body of the article is in English, not Dutch

On Research

- Main objective: Solve open problems

- First become familiar with those problems, existing solutions, and their *limitations*

- Read a lot!

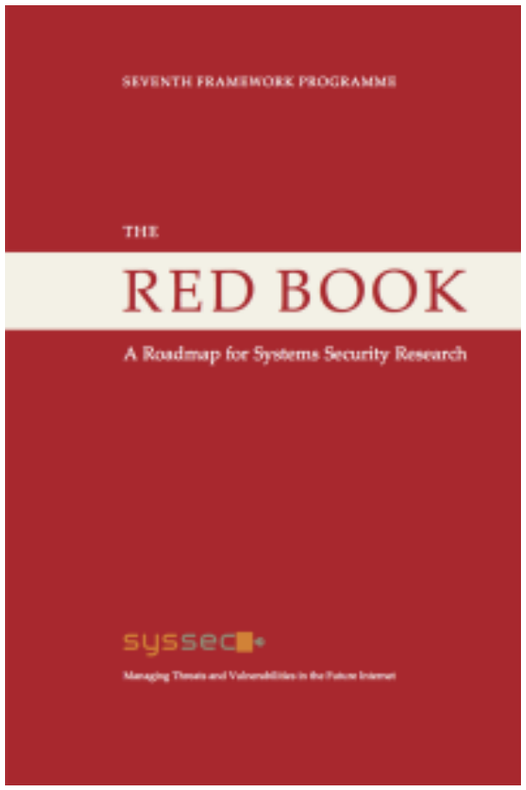
On Research

- Pay attention to *lessons learned* and *future work*
- Write a lot!
- Your advisor will guide you on this journey

Second

Get you a great advisor

A Story in a Story



- “The Red Book: A Roadmap for Systems Security Research” by the SysSec Consortium (published 2013)

On Synergy

- “The whole is greater than the sum of its parts.”
  – Attributed to Aristotle

- Work synergistically with other people

- *Lead and let lead (research projects)*

- Don’t be an island ☺

Skilling Up

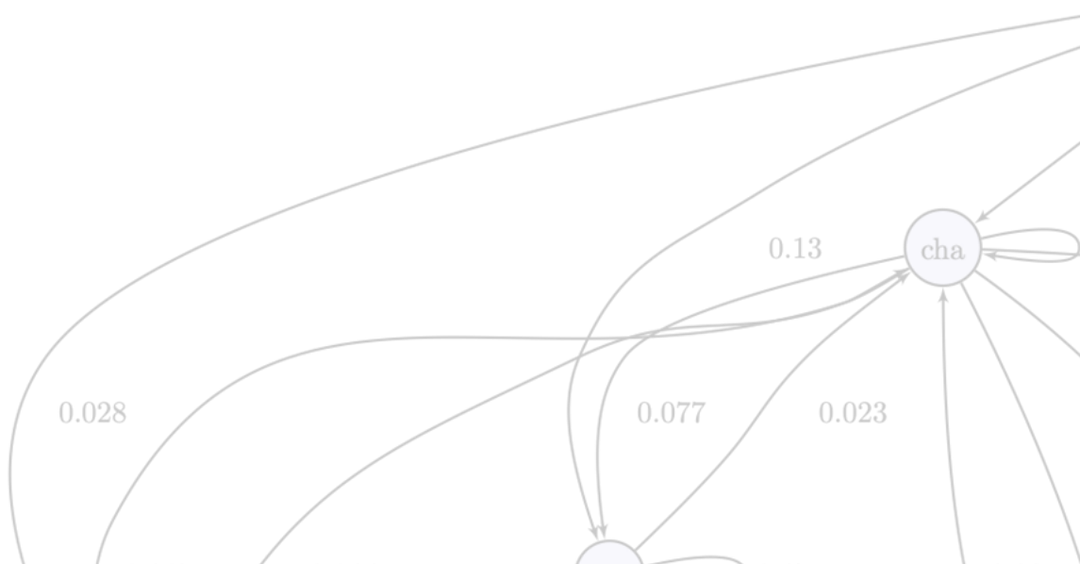
- **Gain new skills!**
- A story in a story:
  - A very Pythonic story (data analysis)
  - Writing and presentation skills—over time
  - Traveling—all expenses paid. Fun!

Making New Friends

Met Snowy the Llama in Perth, Australia (2017). Also saw quokkas, wallabies, emus, and others.

Nowadays

- Assistant Professor at the University of Vermont
- A different quest…the story continues
- Summary: *Demystified* one research journey—you can create/embark on yours, too



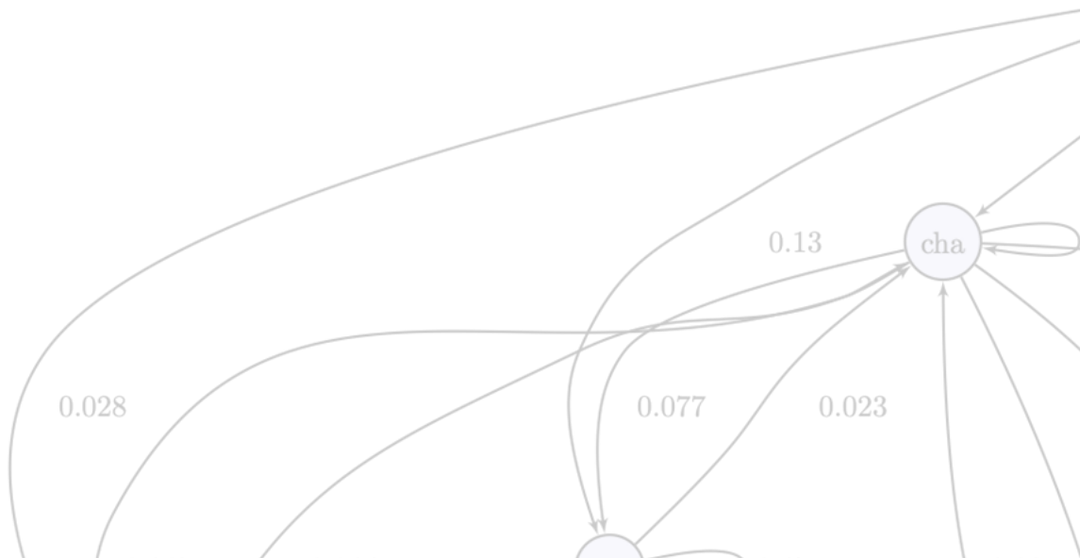
Third

Don’t be an island

Thanks

Many thanks to my family, collaborators, mentors, sponsors/funding agencies, support crew, and everyone who has contributed in a way or another (in no particular order).

You rock!



Thanks

Many thanks to you (yes, *you*) for the gift of your time.

You rock!

Yours truly,

Dr. Jeremiah Onaolapo

https://www.uvm.edu/~jonaolap