black hat USA 2018

AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS

Money-rity Report: Using Intelligence to Predict the Next Payment Card Fraud Victims

Dr. Clare Gollnick, CTO, Terbium Labs
Dr. Cathal Smyth, Sr. Machine Learning Researcher, Royal Bank of Canada

Who We Are?

Terbium labs is a dark web intelligence company made up of an elite group of information security professionals with expertise in everything from cryptography to large-scale information systems.

The Royal Bank of Canada is the largest bank in Canada, and one of the largest in the world (by market capitalization).

Vanguard Cybersecurity Research is a group within RBC with the mission to perform cutting edge research into future cybersecurity threats and innovations.

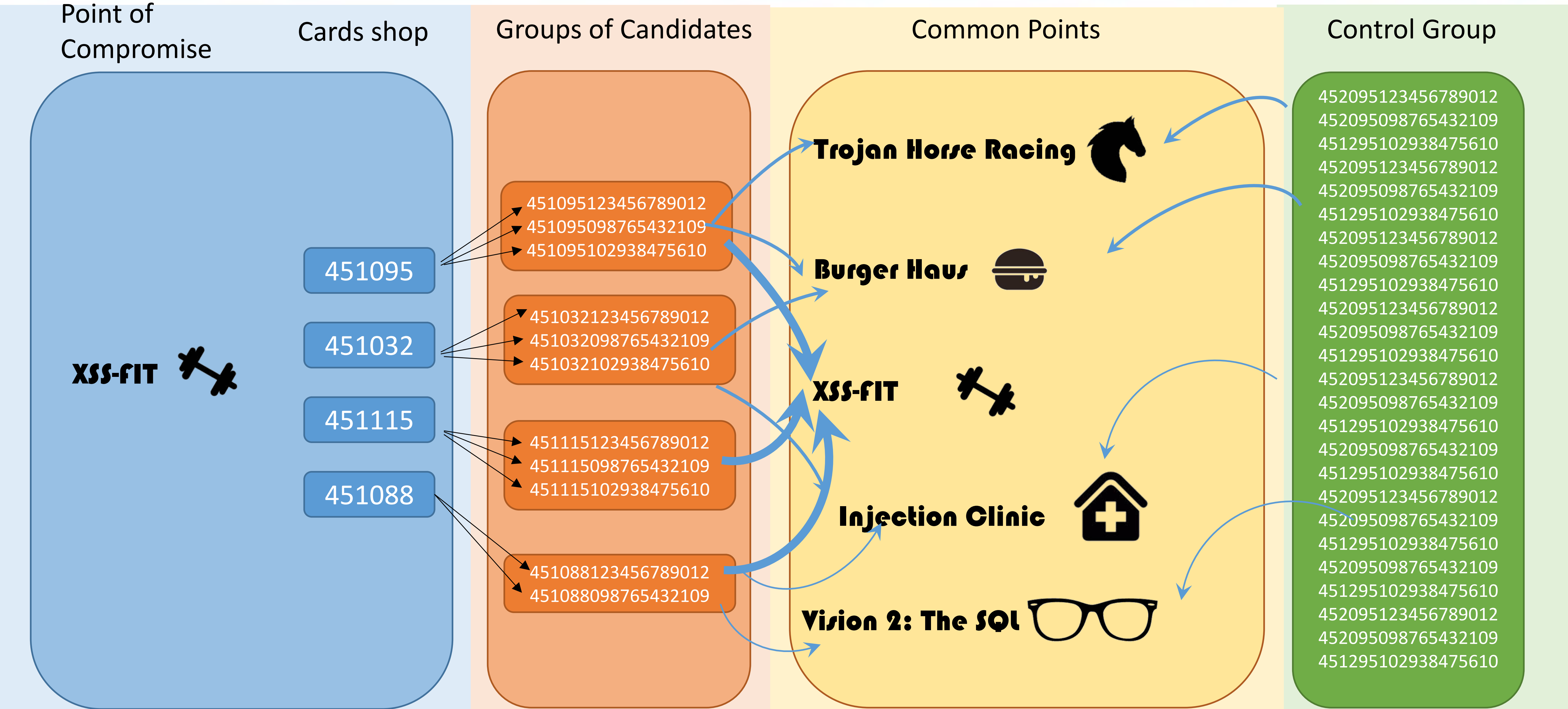
Introduction

- Losses from credit card fraud amount to more than $10 billion dollars annually.
- This money feeds into organized crime, gang activity and terrorism.
- Combatting credit card fraud historically has been a reactionary process.
- By using intelligence gathered from online sources such as the dark web combined with transactional data, we can:
  - identify who the next fraud victims will be
  - where card data is being stolen from
  - before any fraudulent transactions have occurred
  - Without any criminal financing

Traditional Point of Compromise Detection

- Algorithm/Customer/Payment service flags transaction
- Purchase histories of victims are cross-correlated for Common Points of Purchase (CPP).
- List of CPP leads to a Point of Compromise (POC)
- This approach is problematic:
  - Allows fraudsters to purchase and use stolen cards.
  - Requires waiting for more victims to confirm POC.

Dark Web Approach



Point of Compromise

Cards shop

Groups of Candidates

Common Points

Control Group

XSS-FIT

451095
451032
451115
451088

451095123456789012
451095098765432109
451095102938475610

451032123456789012
451032098765432109
451032102938475610

451115123456789012
451115098765432109
451115102938475610

451088123456789012
451088098765432109

Trojan Horse Racing

Burger Haus

XSS-FIT

Injection Clinic

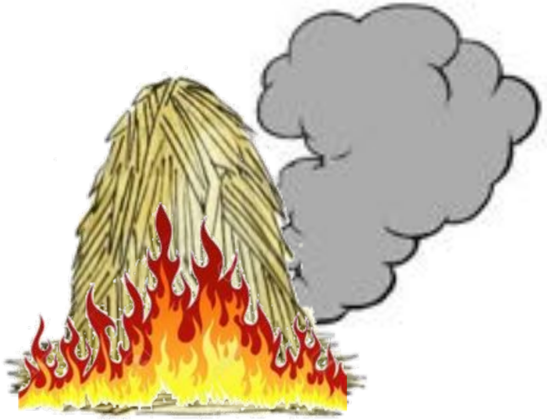
Vision 2: The SQL

452095123456789012
452095098765432109
451295102938475610
452095123456789012
452095098765432109
451295102938475610
452095123456789012
452095098765432109
451295102938475610
452095123456789012
452095098765432109
451295102938475610
452095123456789012
452095098765432109
451295102938475610
452095098765432109
451295102938475610
452095123456789012
452095098765432109
451295102938475610
452095098765432109
451295102938475610
452095123456789012
452095098765432109
451295102938475610

Finding a Needle in a Haystack

- Often a breach can affect a large number of clients.
- Each group can have many candidates.
- Need to find the right combination of clients out of possibly trillions.

Finding a Needle in a Haystack

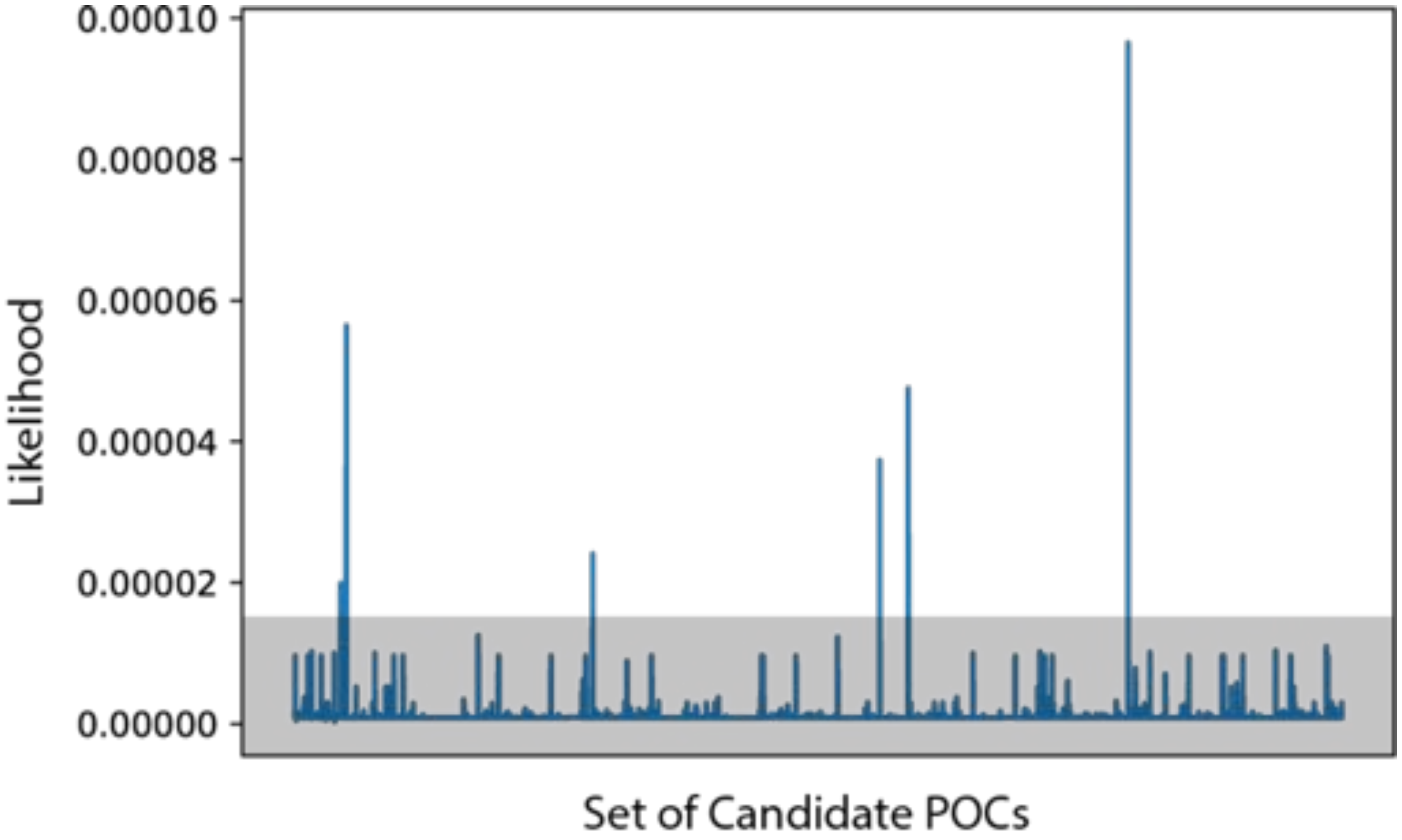


- Set the haystack on fire!
- Ruthless reduction of CPP via various thresholds.
  - The CPP is only shared across less than *g* groups.
  - The popularity of the merchant in the control group is greater than some value *p.*
  - The number of transactions at the CPP is less than *n*.

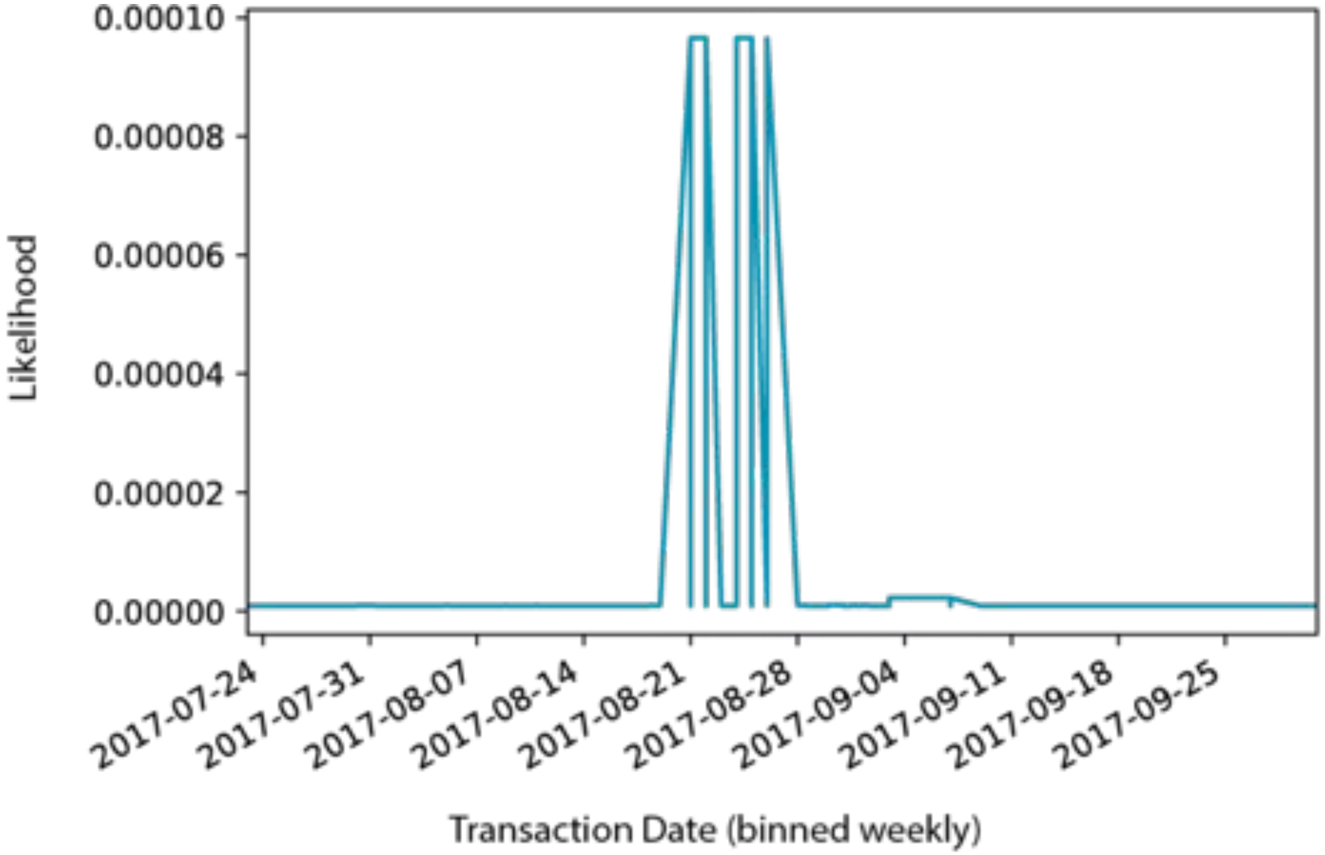
Case Study

- POC spread across ~10 bases.
- Popular restaurant chain – let’s call them “Bob’s”.
- Large impact on many clients.

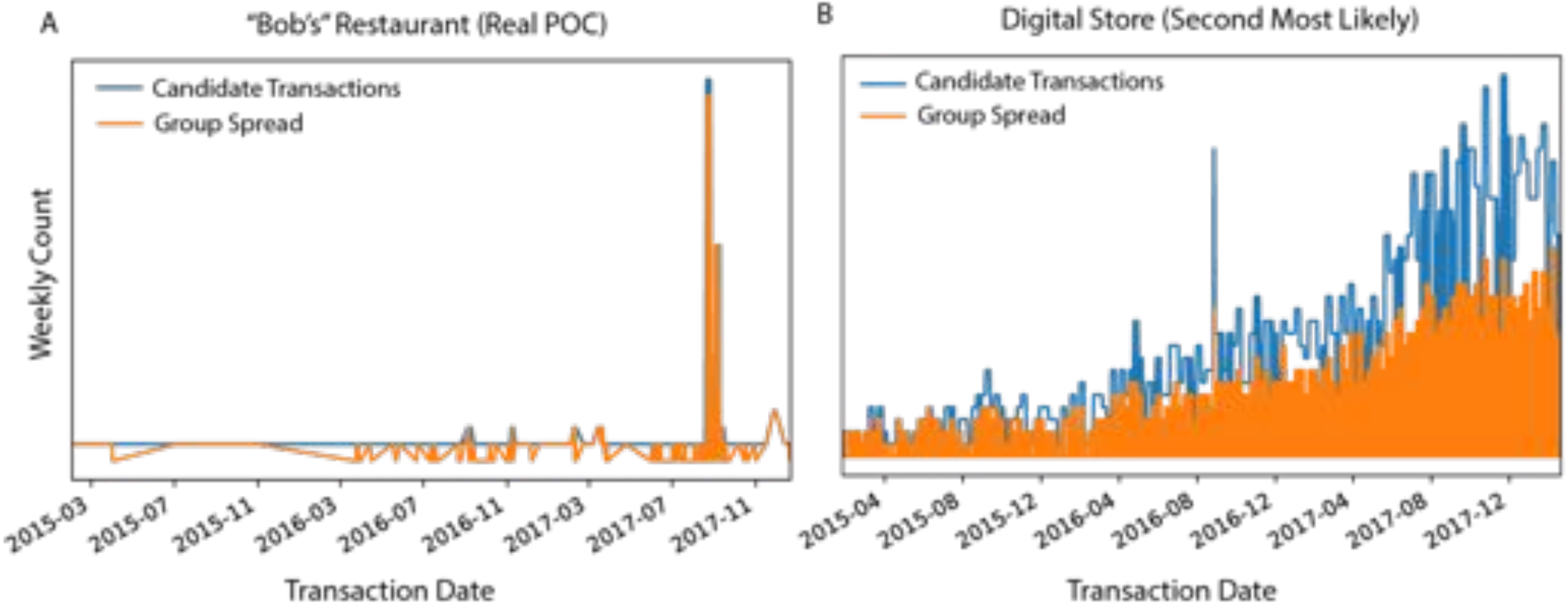
Case Study


0.00010
0.00008
0.00006
0.00004
0.00002
0.00000
Likelihood
Set of Candidate POCs

Case Study


Likelihood
0.00010
0.00008
0.00006
0.00004
0.00002
0.00000
2017-07-24
2017-07-31
2017-08-07
2017-08-14
2017-08-21
2017-08-28
2017-09-04
2017-09-11
2017-09-18
2017-09-25
Transaction Date (binned weekly)

Case Study


A
"Bob's" Restaurant (Real POC)
Candidate Transactions
Group Spread
Weekly Count
2015-03
2015-07
2015-11
2016-03
2016-07
2016-11
2017-03
2017-07
2017-11
Transaction Date
B
Digital Store (Second Most Likely)
Candidate Transactions
Group Spread
2015-04
2015-08
2015-12
2016-04
2016-08
2016-12
2017-04
2017-08
2017-12
Transaction Date

Conclusions

- The dark web enables convenient, one-stop shop selling sensitive information such as credit card details.

- Traditional fraud detection is reactive and permits a thriving criminal ecosystem.

- By leveraging dark web intelligence we can detect data breaches, prevent fraud, and eliminate criminal funding.

Thank You

Danny Rogers
CEO, Terbium labs

Kory Fong
Head of Cybersecurity Research, Royal Bank of Canada

Daniel Swerdfenger
Cyber Analytics Partnerships, Royal Bank of Canada