Infoblox
NEXT LEVEL NETWORKING

Characterizing Certain DNS DDoS Attacks

Andrea Urban, PhD &
Renée Burton, PhD

Introduction

- Who am I?
  - Data Scientist at Infoblox working in the Cyber Intelligence Unit mainly with DNS data
  - Past work
    - Consultant, Professor, Astrophysicist
- What do we do at Infoblox?
  - Detect and Identify Threats in our Customers' Networks
  - Accurate and Specific: Find and Label Attacks

Infoblox®
NEXT LEVEL NETWORKING

THREAT INTELLIGENCE YOU CAN TRUST—ALL IN ONE PLACE

With 10 years of experience, the Infoblox Cyber Intelligence Unit creates, aggregates and curates information on threats to provide actionable intelligence that is high quality, timely and reliable. Threat information from Infoblox minimizes false positives, so you can be confident in what you are blocking, while ensuring unified security policy across the entire security infrastructure.

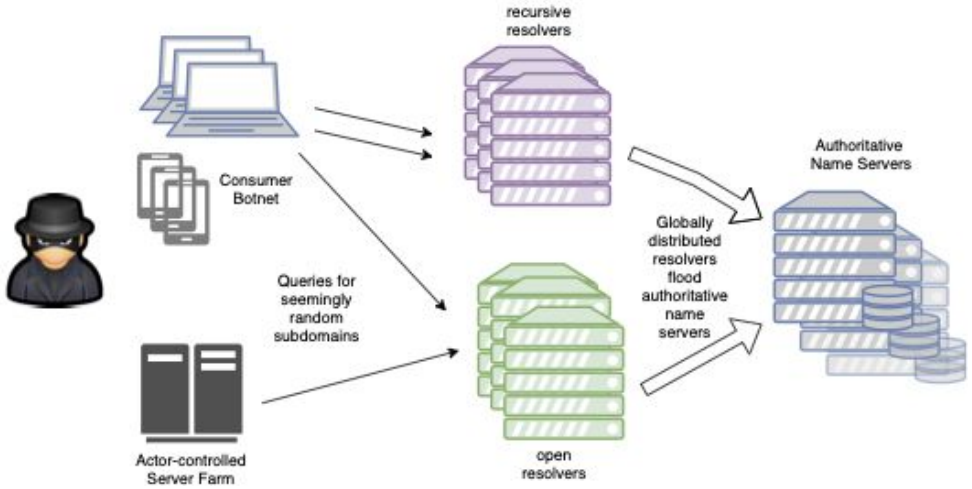
LESS THAN 0.01% FALSE POSITIVES

26+ THREAT INTELLIGENCE PARTNERS

HUNDREDS OF THOUSANDS OF VALUABLE INDICATORS PUBLISHED DAILY

Random Subdomain* DDoS Attacks

- Use “random” subdomains to overload authoritative name servers
  - Resource exhaustion attack
- Attacks against authoritative name servers; domain doesn’t matter really



Goal: Identify and label attacks

We postulate that there are N uniquely identifiable software systems being used in these attacks.

Queries look like:

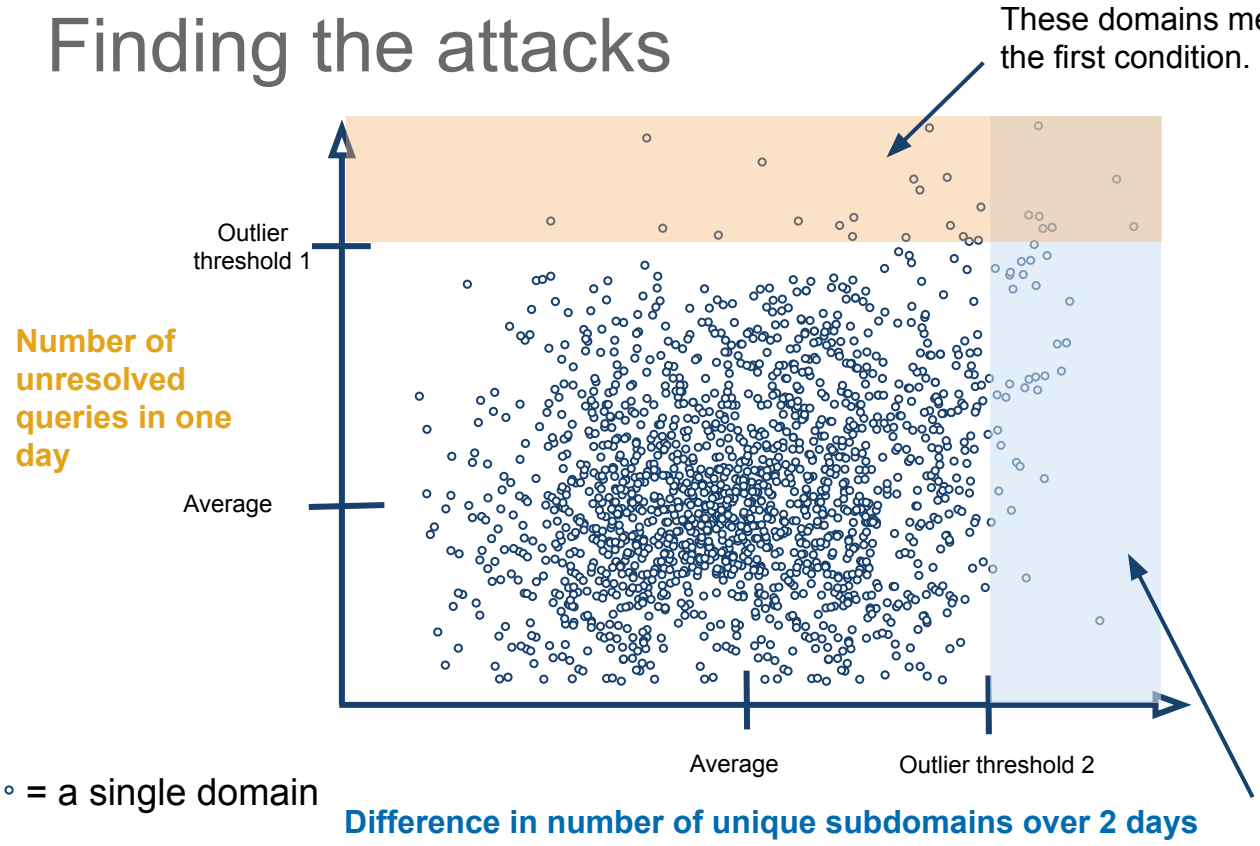
random_prefix.attack_domain

or

random_prefix.fixed_label.attack_domain

* also referred to as Slow Drip or Water Torture DDos attacks

Finding the attacks



◦ = a single domain

Two conditions are used to identify a domain experiencing an attack.

1. Large number of unresolved queries in a day
2. Large increase in number of unique subdomains over past 2 days.

Attacked domains are found in the overlapping region where both conditions are satisfied.

Sample Attack Queries from Various Domains

0k3.hfax.com. 5
t6q.hfax.com. 2
questioned.bjbgp.bjbgp.hfax.com. 2
cxj.bjbgp.hfax.com. 2
lzd.bjbgp.hfax.com. 2
fao.bjbgp.hfax.com. 2
9gi.hfax.com. 1
171j.bjbgp.hfax.com. 1
2ock.bjbgp.hfax.com. 1
krv.bjbgp.bjbgp.bjbgp.hfax.com. 1

us85.91y.com. 10
a34t.bjbgp.91y.com. 7
7c82.91y.com. 3
cp7.bjbgp.91y.com. 2
01uq.bjbgp.91y.com. 2
uh5t.bjbgp.91y.com. 2
dwu9.91y.com. 2
g1we.91y.com. 1

qiv.wan.douyu.com. 3
worst.bjbgp.g.wan.douyu.com. 3
2xqy.passport.douyu.com. 3

i92.skeeball-arcade.scopely.com. 1
china.scopely.com. 1
books.scopely.com. 1
deal.yahtzee-with-buddies.scopely.com. 1
songs.tech.scopely.com. 1
gw2.wheel-of-fortune.scopely.com. 1
ab4.scopely.com. 1

Queries USED TO look like:

random_prefix.attack_domain

or

random_prefix.fixed_label.attack_domain

- Prefix isn't random; can contain dictionary words.
- Fixed label is no longer fixed. Can vary.

The problem

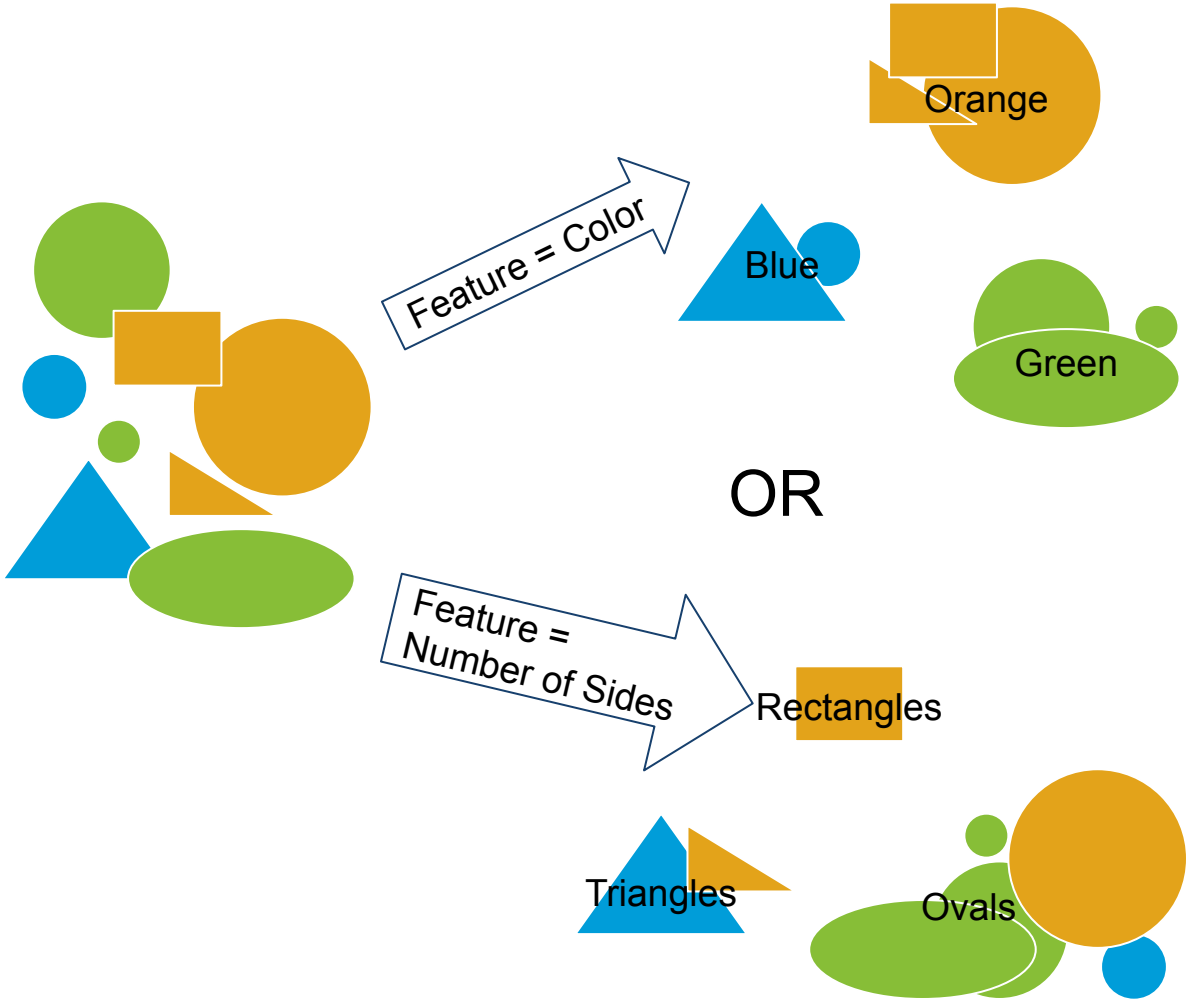
- take ~800M records like the ones on previous slide
- put them into buckets of attacks generated by the same malware
- where an attack is (date, domain)

The solution

- use machine learning: “unsupervised learning” technique can cluster, or group, attacks that have similar “features”

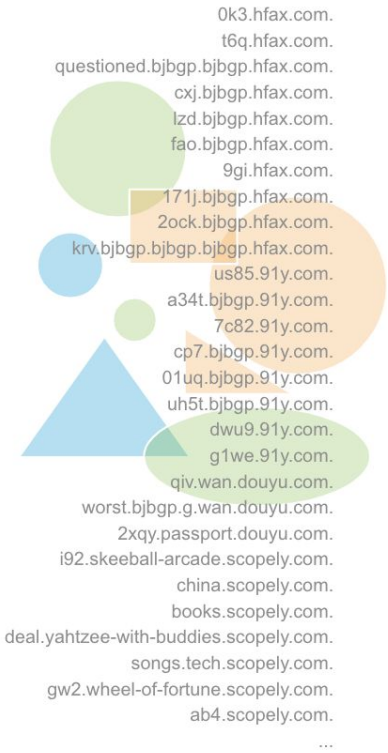
Machine Learning

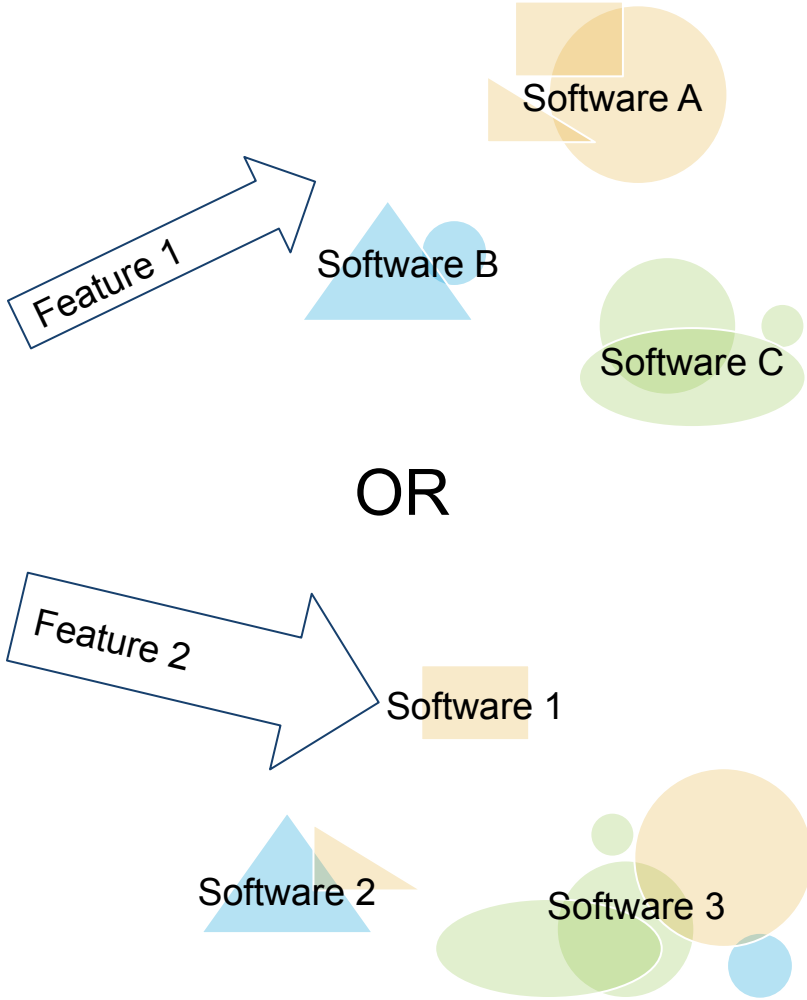
- Features of the data
  - Color, Size, Number of angles, Number of sides
- Unsupervised Machine Learning
  - Train the model to group similar things together
  - Depends on the features chosen or the question you are asking.



Machine Learning

- Problem is hard: we don't have sample malware.
- Features we can explore
  - Landscape statistics
  - Qname statistics
  - Similarity statistics
  - Time series analysis
  - …..
- Strong clustering will require **many** features.
- Showing just 2 features in detail today.



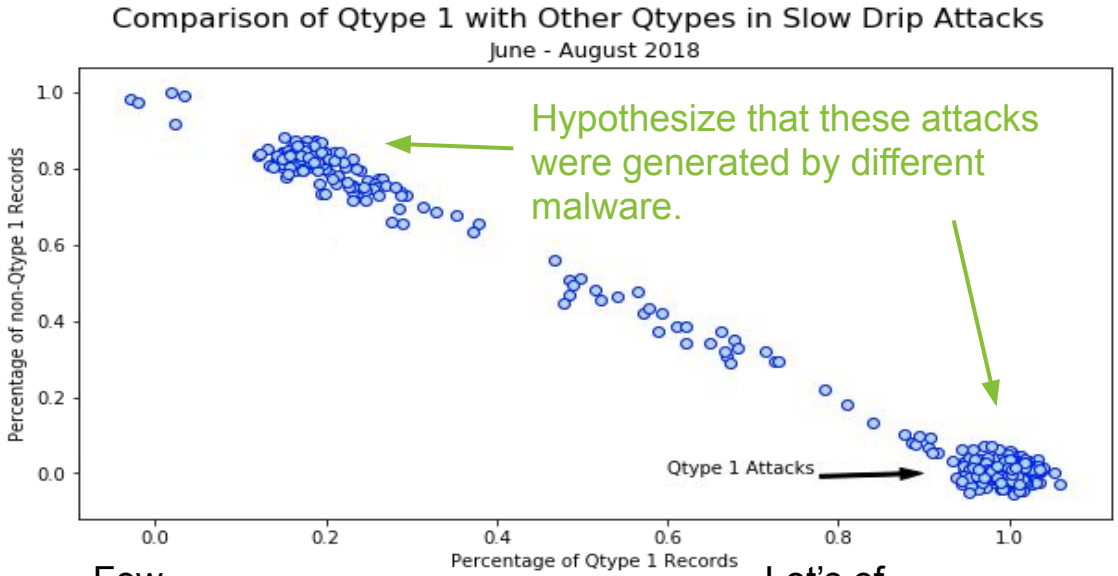


 |

Feature 1: Query Type

Data set

- 444 attacks occurring over ~75 days

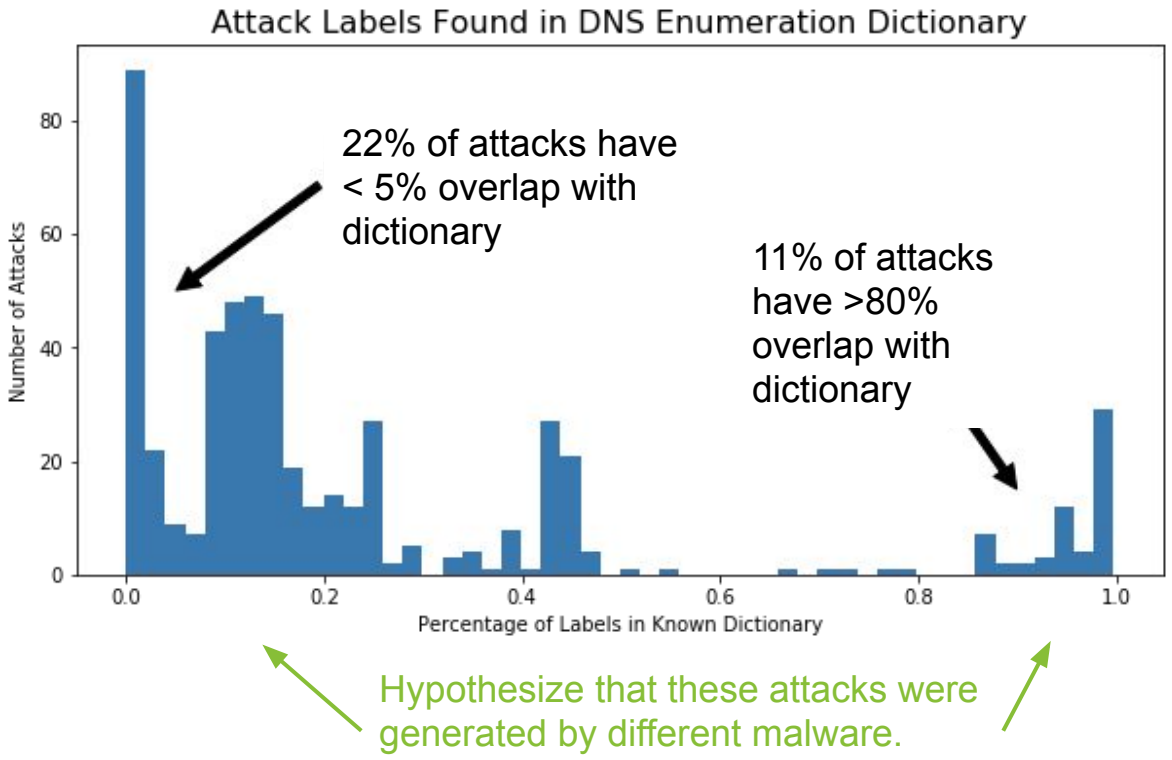


Few
Qtype = 1 records

Lot's of
Qtype=1 records

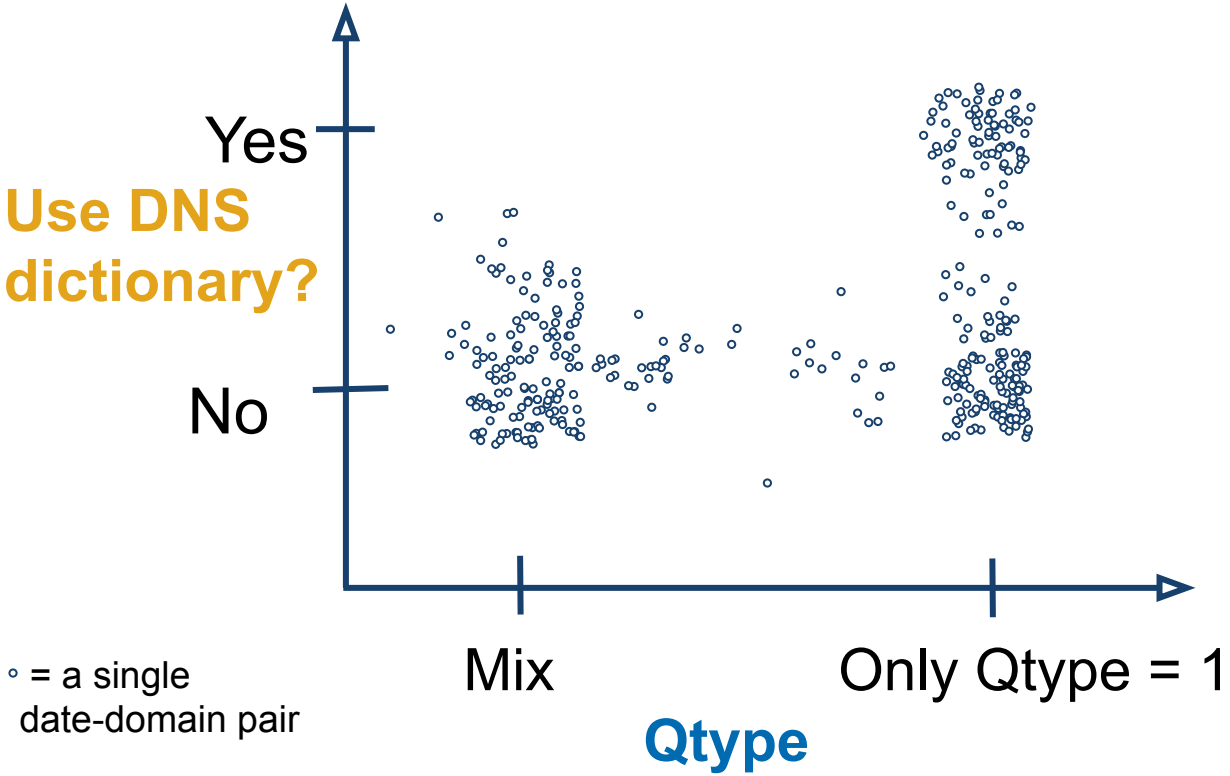
Feature 2: DNS Enumeration Dictionary

- A substantial number of the attacks use a dictionary for generating their random subdomain strings.
  - Google shortcut to reverse engineering
  - Github dictionary text file contains ~420k words



 |

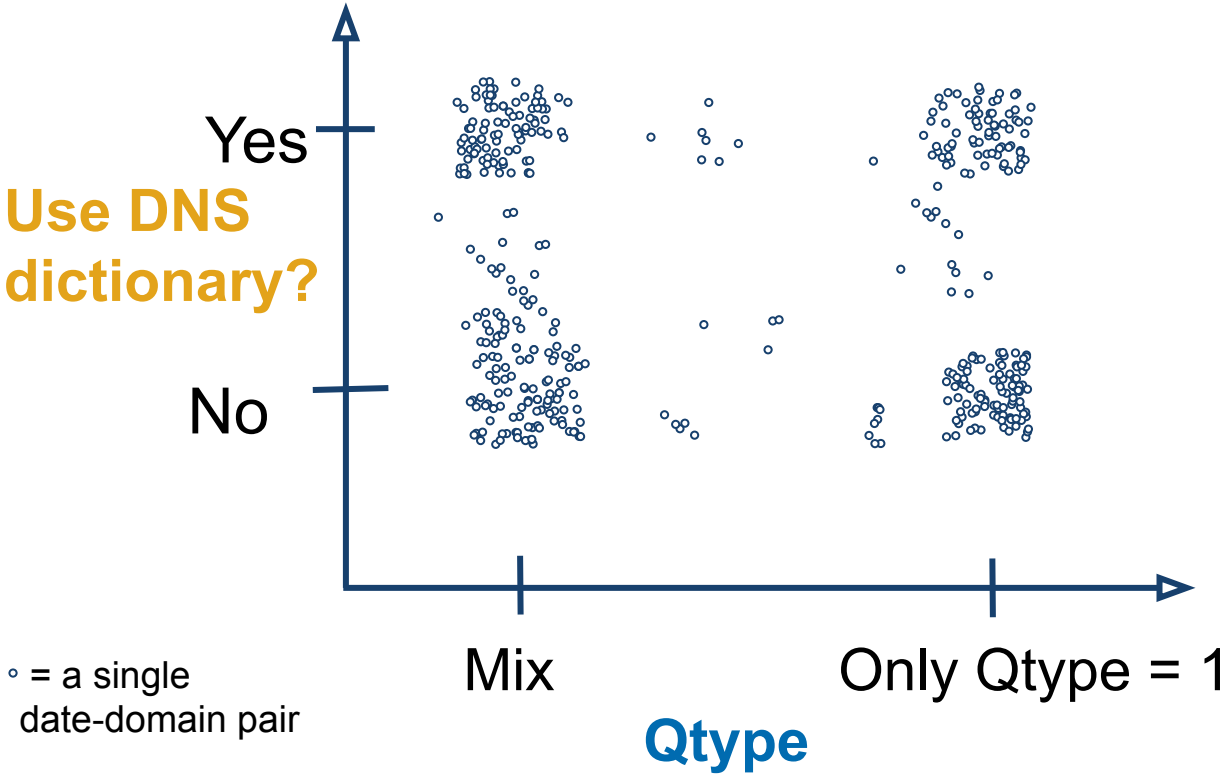
Grouping the attacks



How many malware systems are creating these attacks?

3?

Grouping the attacks

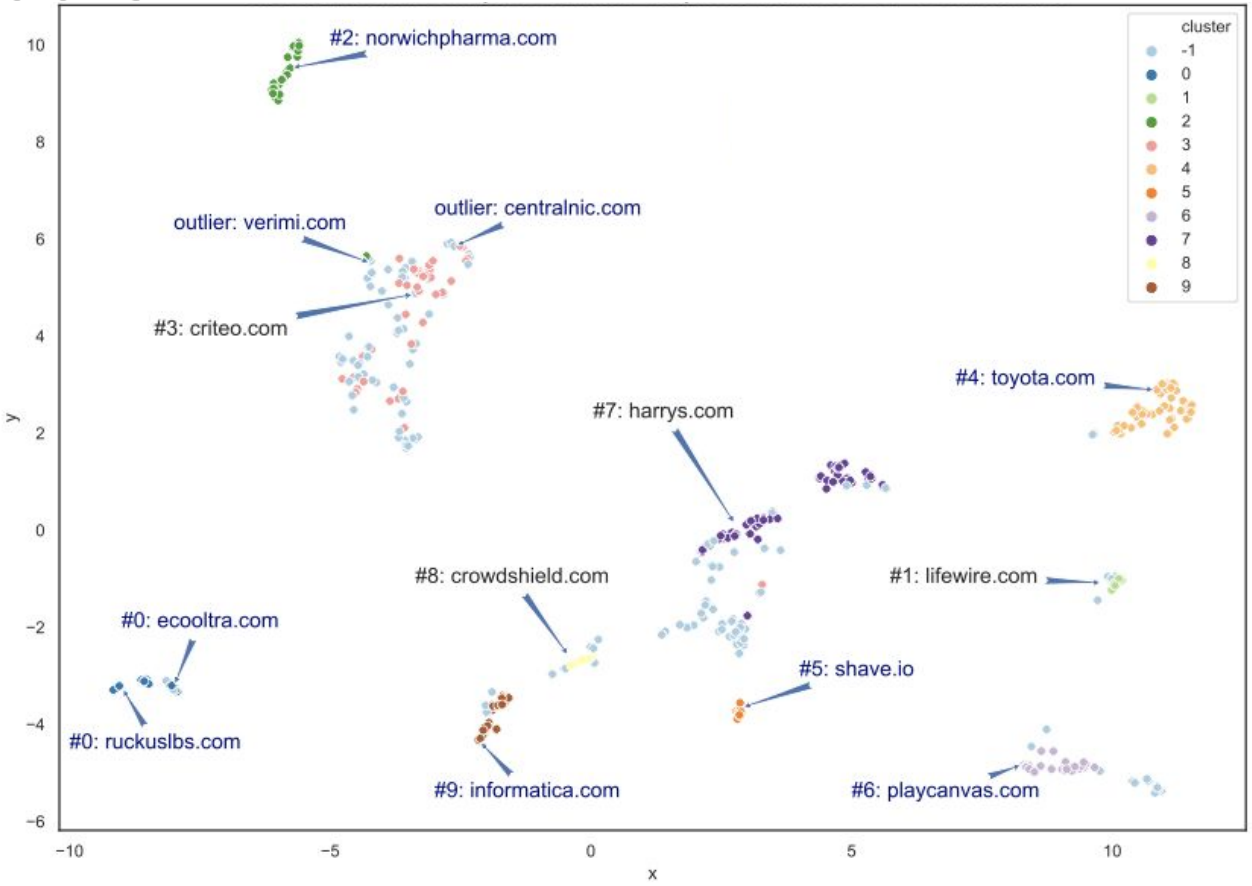


How many malware systems are creating these attacks?

4?

Clustering the Attacks

- 20 Features in Total
  - Percentage of qtypes
  - Dictionary overlap
  - Character distributions
  - Time series
  - Percentage of unique labels in attack
  - Mean prefix lengths
  - etc.
- Used HDB-SCAN to cluster attacks in 20 dimensions
- Use UMAP to project 20-dimensional space into 2-d plane
  - -1 indicates an outlier



 |

Cluster properties

From 20 features, we are able to group attacks into about 8 clusters, which are different from original attack profile.

It is *unlikely* that one single piece of malware is generating these new attacks, unlike previous attacks.

Using these groups, it's possible to track the evolution of the malware systems over time.

No.	Size	Days	Sample Attack Domains	Dominant Features
0	20	6	AirBnB-related, Ruckus Wireless	high DNS overlap, five qtypes, lex-ascending, moderate attack lengths
1	11	5	DotDash-related	redundant labels, one qtype, high DNS enumeration overlap, short attacks
2	28	5	Pharmaceutical Industry and Icelandic	unique labels, lex-descending, five qtypes, moderate length attacks
3	46	28	Indonesian domains, universities, payment sites, Tinder	very lex-ascending, five qtypes
4	47	19	Toyota, Starbucks, Paypal	high label reuse, high DNS overlap, one qtype
5	10	9	`dollarshaveclub.com`, `shave.io`	no DNS enumeration overlap, one qtype, strong unigram pattern, shorter attacks
6	27	8	starting `sc-`, AirBnB-related, PlayCanvas	moderately duplicated labels, one qtype, no DNS enumeration overlap, lex-ascending, strong unigram pattern
7	55	12	Western Union, Harrys	~50% label reuse, one qtype, short attacks, high lex-ascending
8	11	6	`crowdshield.com`, `coupa.com`	one qtype, high lex-ascending, far from unigram models

Conclusions

Threat landscape has changed. Simple random subdomains are no longer the norm. More complicated behavior is emerging. More than one actor/malware system is active.

- Multiple query types are becoming more common.
- Uniform random prefixes are no longer prevalent, rather dictionary-generated are more common

Attack generators could be combining techniques for creating qnames.

Monitoring attacks that fall outside these clusters could give indications of changing attack tactics.

Paper with more details: https://arxiv.org/abs/1905.09958


Thank You
Asante
Shukria
Dhanyavadagalu
Vinaka
köszönöm
Kiitos
Maake
Manana
Dankon
Kam Sah Hammida
Matondo
Terima Kasih
Taiku
Tack
Dank Je
Dankscheen
спасибо
Mauruuru
Biyan
Chokrane
Diolch i Chi
Blagodaram
Ngiyabonga
Dziekuje
Grazie
Arigato
Juspaxar
Mochchakkeram
Gracias
Tingki
Paldies
Bedankt
Dakujem
Gratias Tibi
cảm ơn bạn
Grazas
Ua Tsaug Rau Koj
Obrigado
Khun Khap
Kop
Kia Ora
Děkuji
Nirringrazzjak
Suksama
Di Ou Mèsi
Hvala
Djiere Dieuf
Welalin
Danke
Go Raibh Maith Agat
Eskerrik Asko
Najis Tuke
Salamat
Merci
Misaotra
Rahmat
Nuwun
Matur
谢
谢
хвала
ขอขอบคุณคุณ
ありがとう

Extra slides

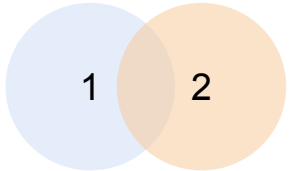
Finding the attacks

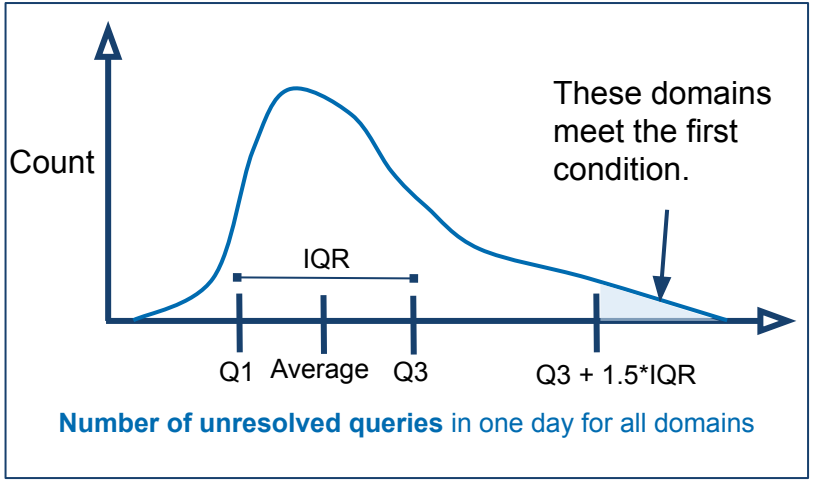
Two conditions are used to identify a domain experiencing an attack.

1. Large number of unresolved queries in a day

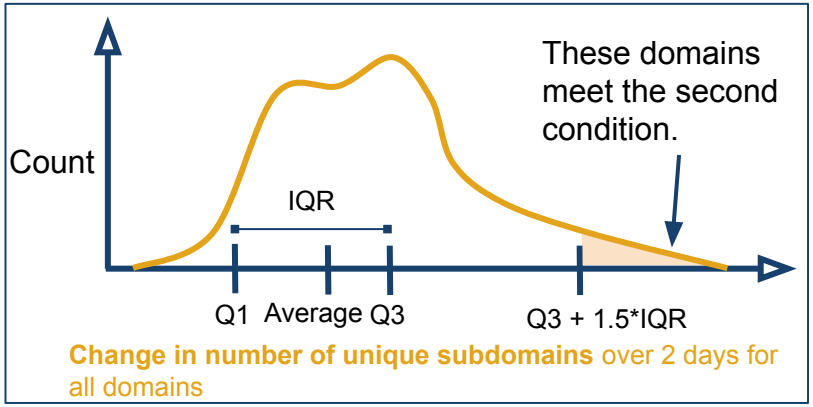
2. Large increase in number of unique subdomains over past 2 days.

Attacked domains are found in the overlapping region where both conditions are satisfied.





Number of unresolved queries in one day for all domains



Change in number of unique subdomains over 2 days for all domains

 |