RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PDAC-R01

# What Was Once Old Is New Again: Domain Squatting in 2020

**Jeremy du Bruyn**
Practice Manager
Sense of Security
@herebepanda

**Willem Mouton**
Head of Research
Sense of Security
@_w_m__

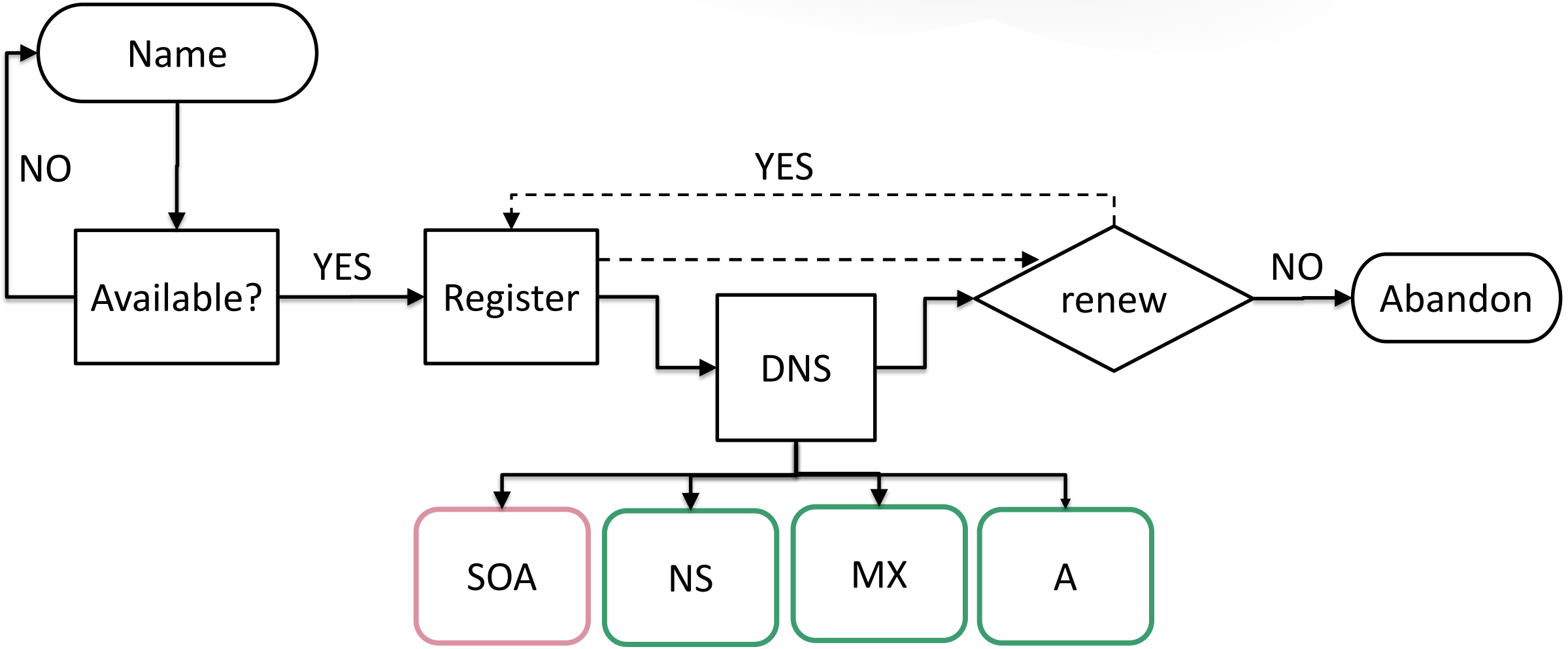
# Agenda

- Story 1: The adventure
  - An introduction to domain squatting and our work to quantify how big of a problem it is.
- Story 2: A cautionary tale
  - How we used domain squatting to gather tons of useful information during our red team exercises.

RSAConference2020

# Introduction: Domain Squatting 101

# Domain Registration Process



# Domain Squatting: Goals

## Financial Gain

- Sell domain
- Advertising
- Affiliate programs
- …

## Maliciousness

- Phishing
- Malware
- Information leakage/gathering
- …

# Domain Generation methods

- Typosquatting
- TLD “substitution”
- “Missing-dot”
- ”Combo”
- Homoglyphic
  - à, ğ, ẘ
- Abandoned domains
- Homophones
  - bobs-oars.com = bobs-ores.com

# FYI: goolge.com

## Whois Record for Goolge.com

**Domain Profile**

| | |
|---|---|
| **Registrant Org** | Google LLC |
| **Registrant Country** | us |
| **Registrar** | MarkMonitor, Inc. MarkMonitor Inc.<br>IANA ID: 292<br>URL: http://www.markmonitor.com<br>Whois Server: whois.markmonitor.com<br>abusecomplaints@markmonitor.com<br>(p) 12083895770 |
| **Registrar Status** | clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited |
| **Dates** | 7,566 days old<br>Created on 1999-06-04<br>Expires on 2020-06-04<br>Updated on 2020-01-14 |
| **Name Servers** | NS1.GOOGLE.COM (has 12,599 domains)<br>NS2.GOOGLE.COM (has 12,599 domains)<br>NS3.GOOGLE.COM (has 12,599 domains)<br>NS4.GOOGLE.COM (has 12,599 domains) |

RSAConference2020

# Chapter 1: The Journey Begins

# Some questions we had

- How many domain squatting domains are there?
- Just how big a problem is domain squatting?

# The targets


London
Stock Exchange
TMX
Toronto Stock
Exchange
NYSE
Nasdaq
BSE
EXPERIENCE THE NEW
HKEX
香港交易所

# The targets

4,478 targets

3,126 DNS domains

# Our approach v0.1

- Sourced 247+ million registered domains
- Squatting categories:
  1. Typosquatting – (Levenshtein distance)
  2. TLD “substitution” (1550+ TLDs)
  3. “Missing-dot” (wwwexample.com)

# Levenshtein distance

- Words/domains within 1 “edit” of a target domain

1.....0.....1

xample.com example.com examples.com

# Finding the squatters

- 267,634 possible squat domains identified
  - Typosquatting : 173,512
  - TLD “substitution” : 92,890
  - “Missing dot” : 1,232
- A LOT were legitimate, so we needed to differentiate
  - abc.com is not a squat of abb.com

The journey begins…

RSAConference2020

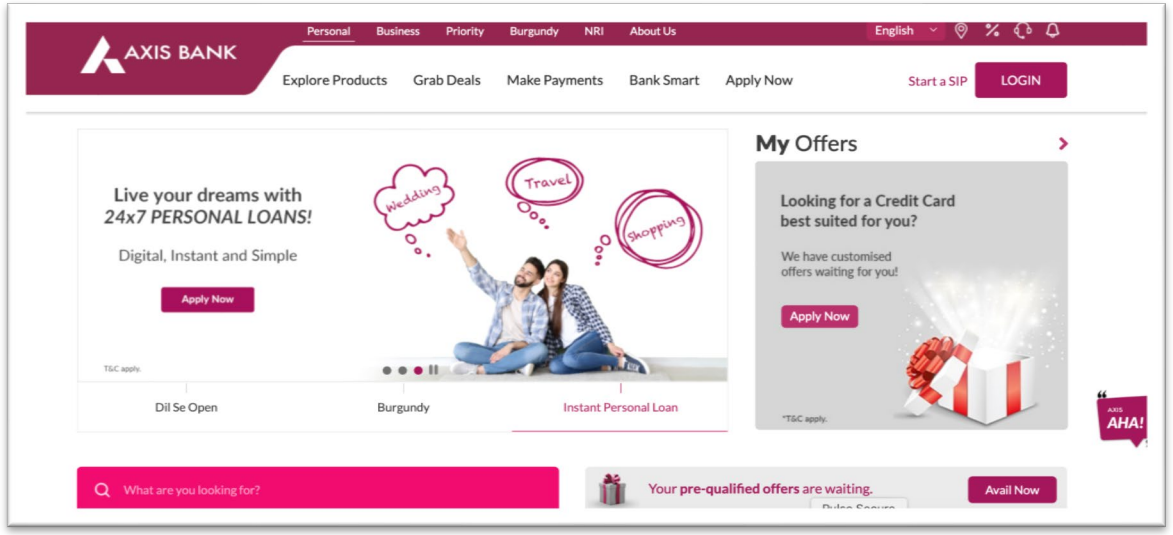
# Chapter 2: Categorisation

# Let's get with the categories

- Categorised all 267,634 domains
- Manually verified 1000's
- Many, many false-negatives
- Cannot use domain categorization alone

# Not always correct

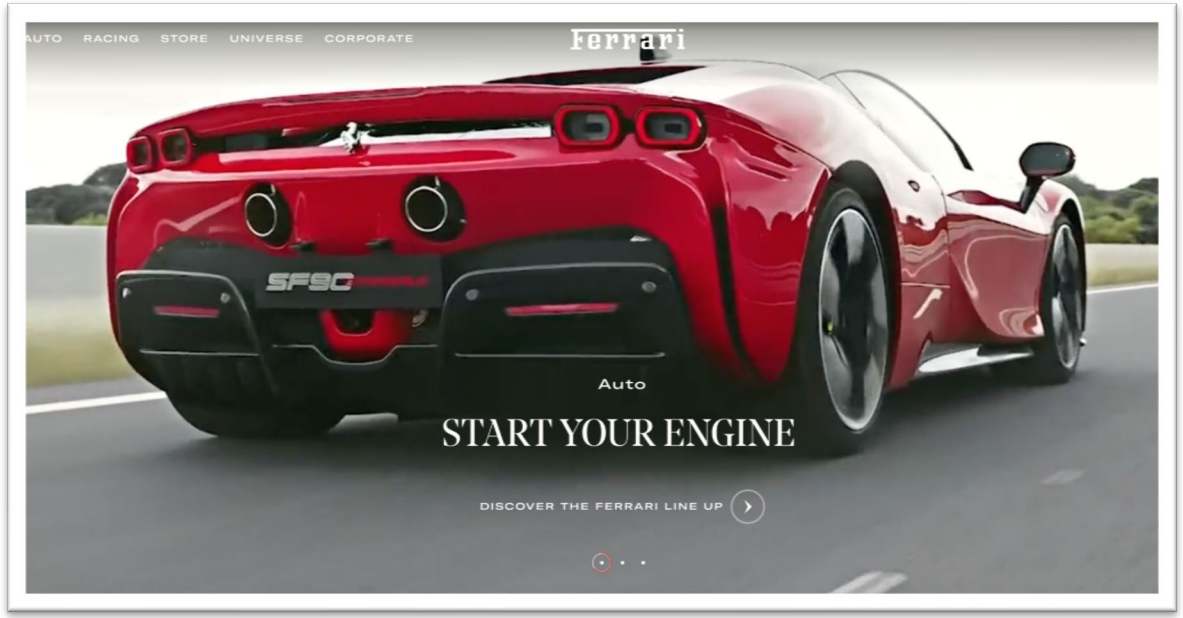
## Banking and Finance



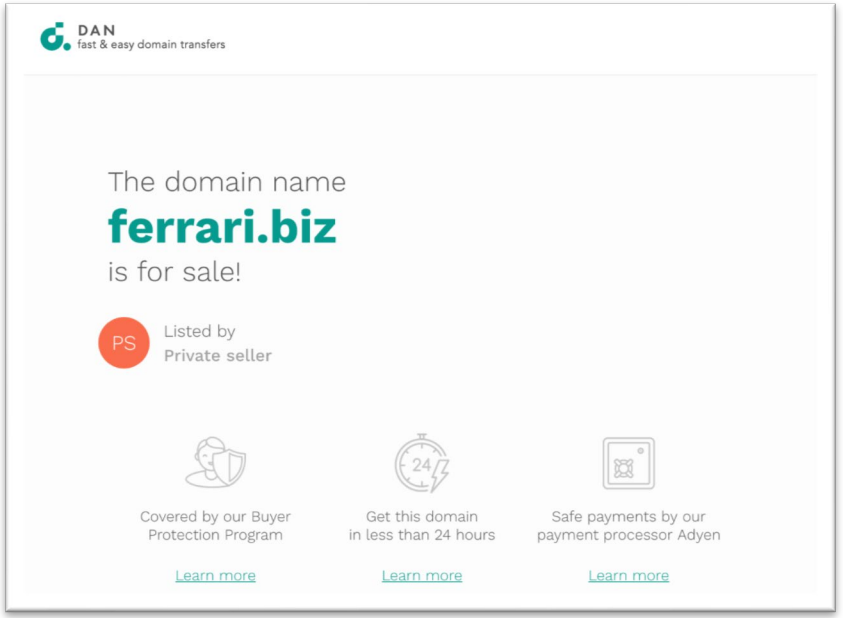

## Business

# Although sometimes…

## Personal Vehicles



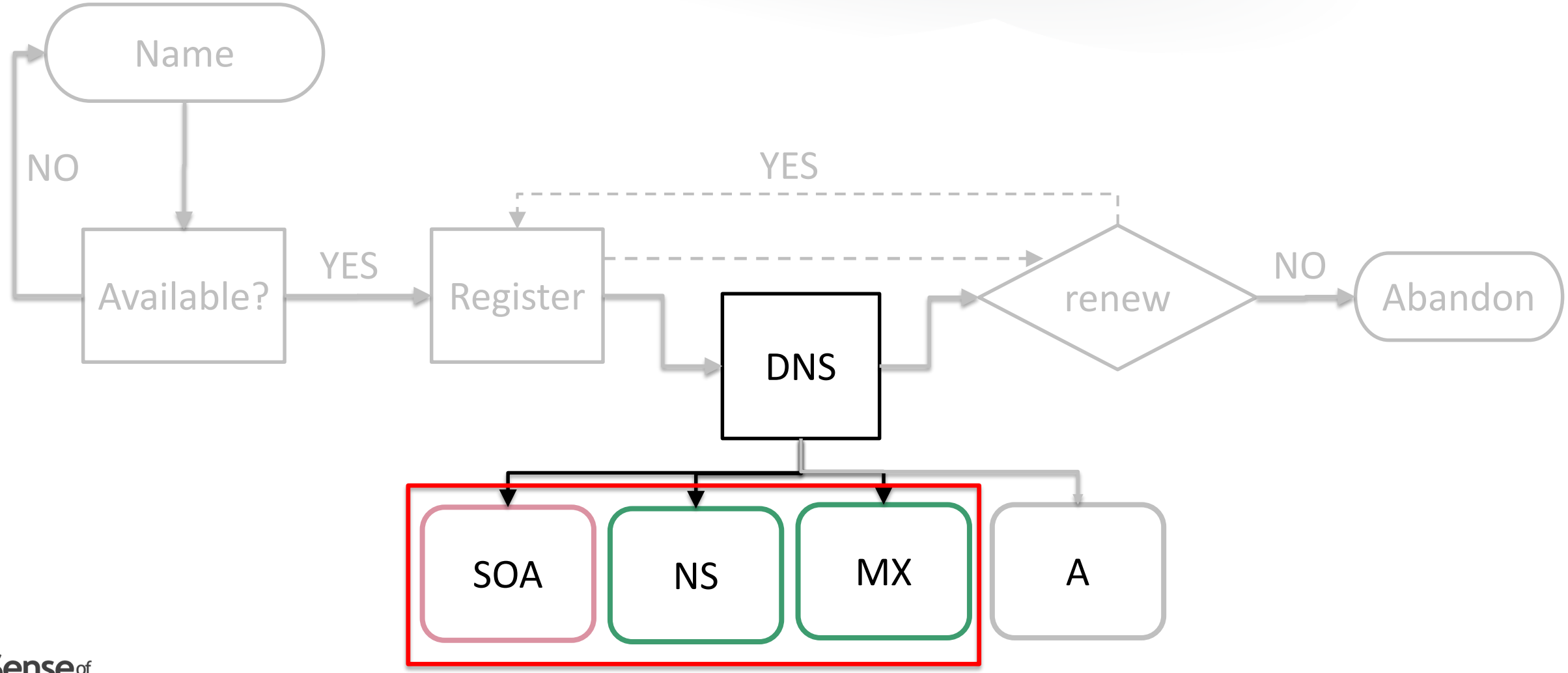

## Spam URLs



RSAConference2020

# Chapter 3: DNS

# Records collected



# DNS Totals

| | |
|---|---|
| Start of Authority (SOA): | 268,130 |
| Name servers (NS) : | 757,981 |
| Mail Exchangers (MX): | 1,053,492 |
| Grand Total: | 2,079,603 |

# Largest DNS SOA providers

1. namebrightdns.com
2. uniregistrymarket.link
3. sedoparking.com
4. parkingcrew.com
5. dns.com
6. bodis.com
7. cscdns.net
8. registrar-servers.com

# Verification

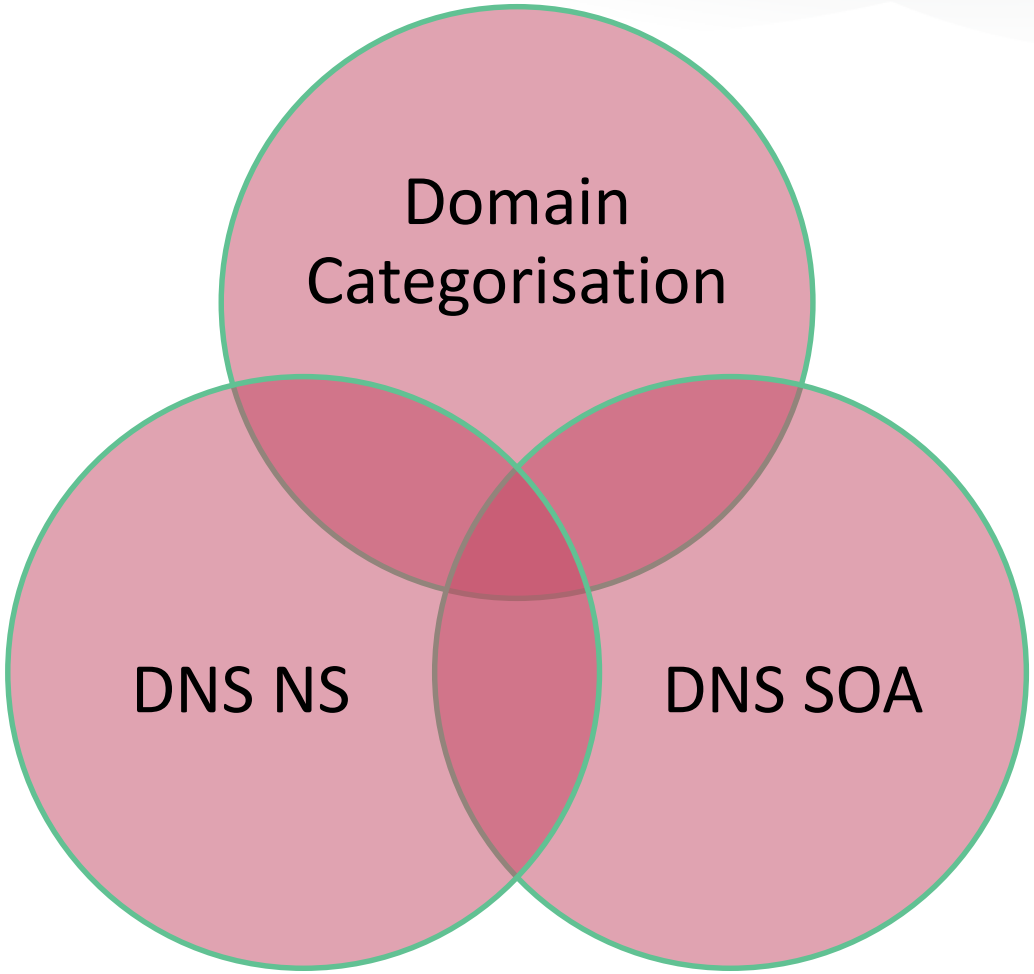
- Again cross-referenced results with screenshots
- More false-negatives
- Squatters don’t all congregate on known “bad” DNS servers
- Squatters also host on “good” DNS servers

We venture forth….

RSAConference2020

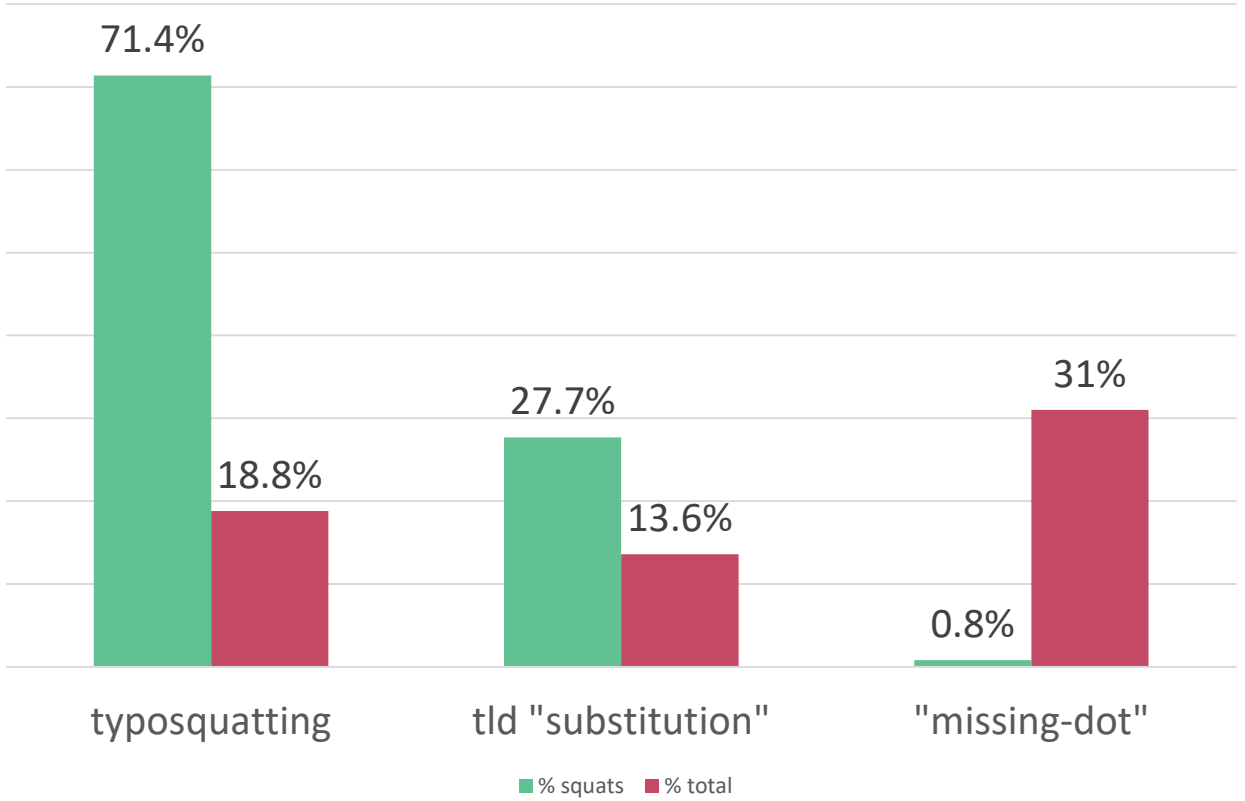
# Chapter 4: Intersection

# Correlation



# Confirmed squatting domains

- Conservatively identified 45,646 domains
  - Approximately 17% of the total domains



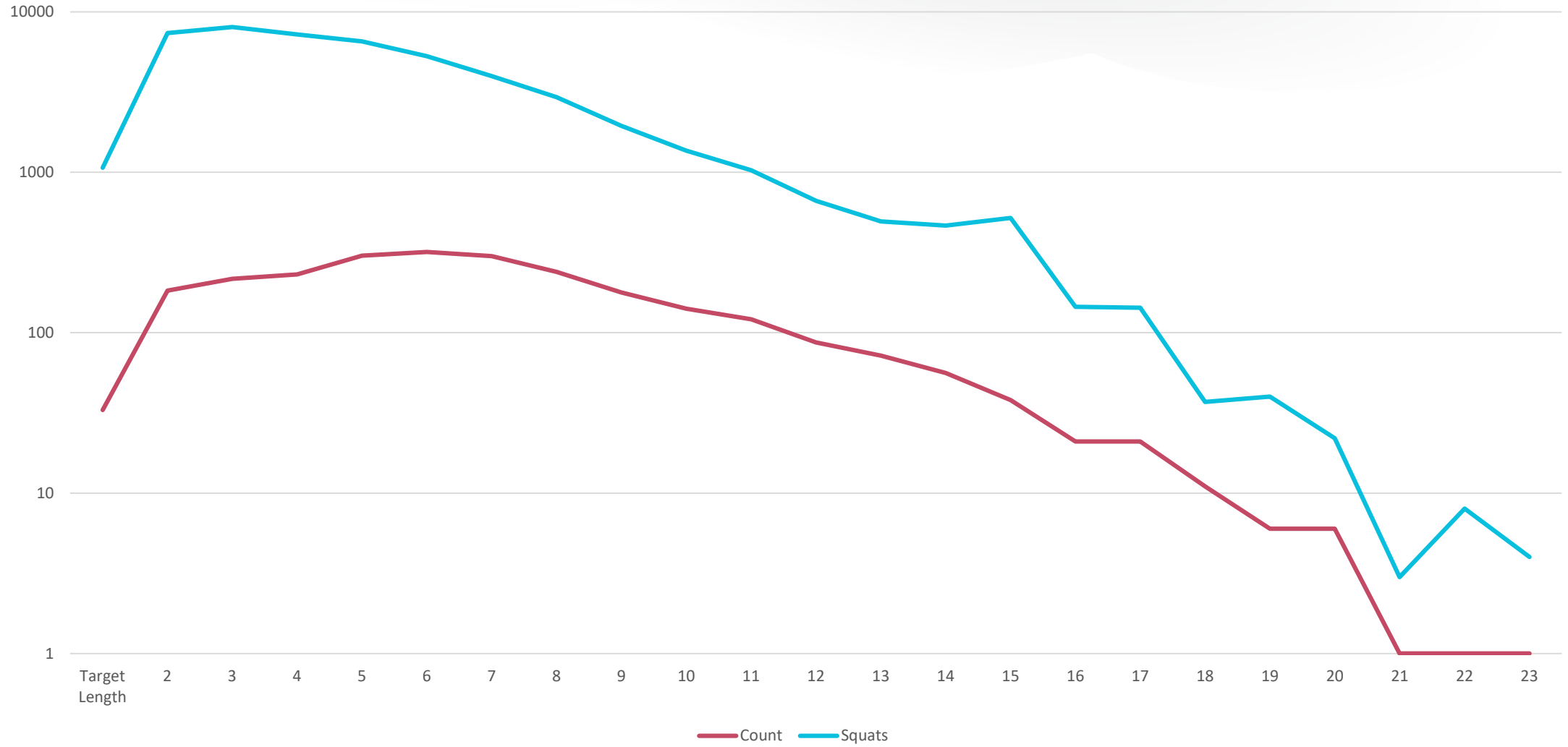
# Largest DNS SOA squat providers

1. uniregistrymarket.link.
2. sedoparking.com.
3. parkingcrew.net.
4. dns.com.
5. above.com.
6. bodis.com.
7. parklogic.com.
8. name-services.com.
9. domaincontrol.com.

# Top 10 squatted organisations

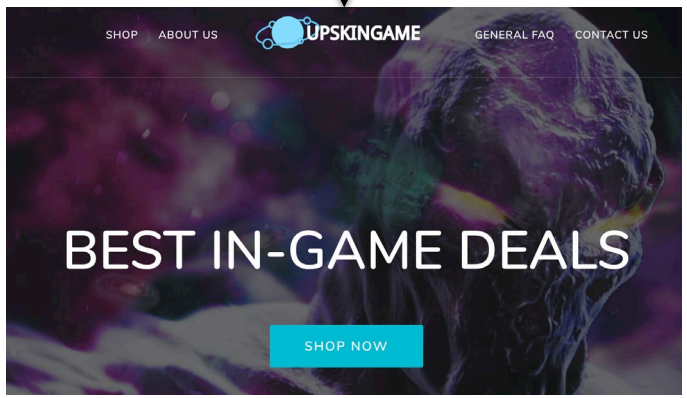
1. Ares Management (aresmgmt.com)
2. Fogo de Chão (fogo.com)
3. Facebook (facebook.com)
4. Quantum Corporation (quantum.com)
5. Zillow (zillow.com)
6. Coupons.com (coupons.com)
7. Progressive Corporation (progressive.com)
8. Uber (uber.com)
9. The Hartford (thehartford.com)
10. United Airlines Holdings (united.com)

# Domain Length: Counts and Squats

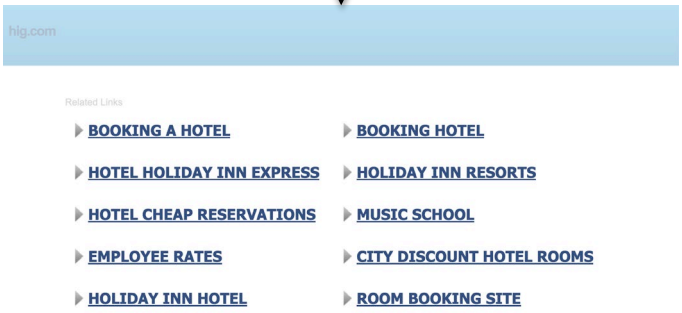


# Umbrella Popularity List—Top Million Domains


Rank #214,070







RSAConference2020

# Chapter 5: Conclusion

# Remember for later…

Squat domains with MX records: 23,131 (~50%)

# Lessons learned

1. Using Levenshtein distance is useful, but expect a lot of data
2. It's difficult to tie a squatting domain back to a specific target
3. It's even more difficult to identify the actual owner of the squatting domain
4. Domain categorisation is not an exact science
5. DNS domains change OFTEN (duh)
6. Squatters employ some creative techniques to hide their infrastructure

# Future work - v0.2

- Go bigger:
  - Targets (more stock exchanges)
  - Squat types (combo, abandoned, etc.)
  - Domains list (250 million is not enough)
- Continuous analysis, not point in time
- “Faster” domain categorisation system
  - We played nice, but need something that scales
- Include more features (screenshots, ssdeep, keywords)

RSAConference2020

# A Cautionary Tale:
# Red Team domain squatting

RSAConference2020

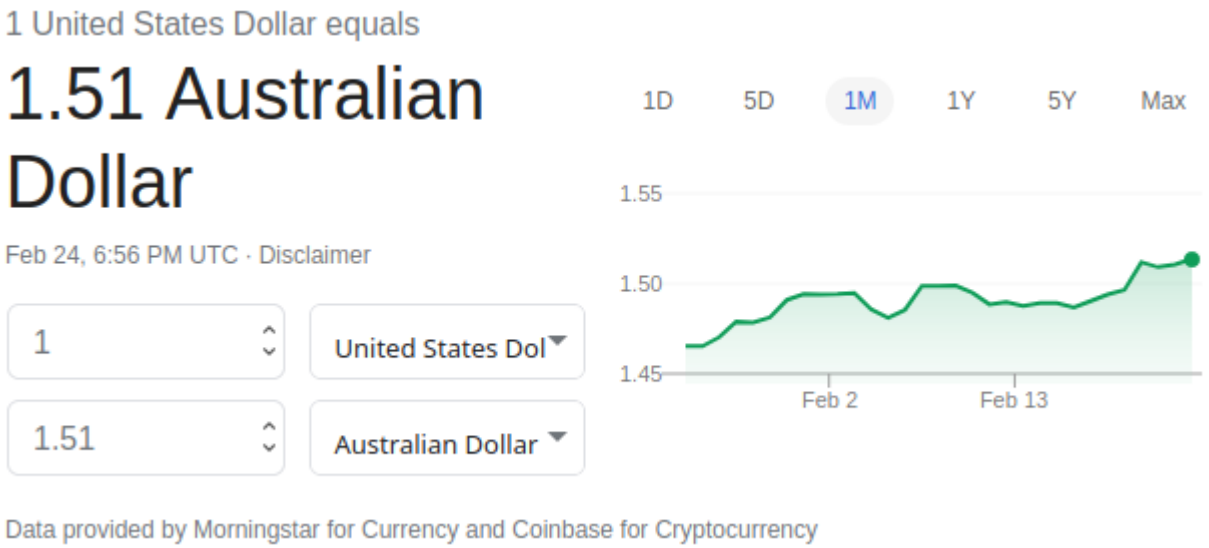
# Chapter 1: The Quest for Treasure

# Goals

- Find a more intelligent way of identifying useful squatting domains, not as much brute force
- Capitalize on mistakes made by clients and employees
- Gather data passively
  - Email behavior
  - Types of data sent / received
  - Supply chain interactions
  - Contextual information used for social engineering

# Problems needed solving

- Large number of candidate domains
- Traditional obvious ones already taken
- Budget of AU$20 ☺ (That's Aus $$)



RSAConference2020

# Chapter 2: Red Team 2019

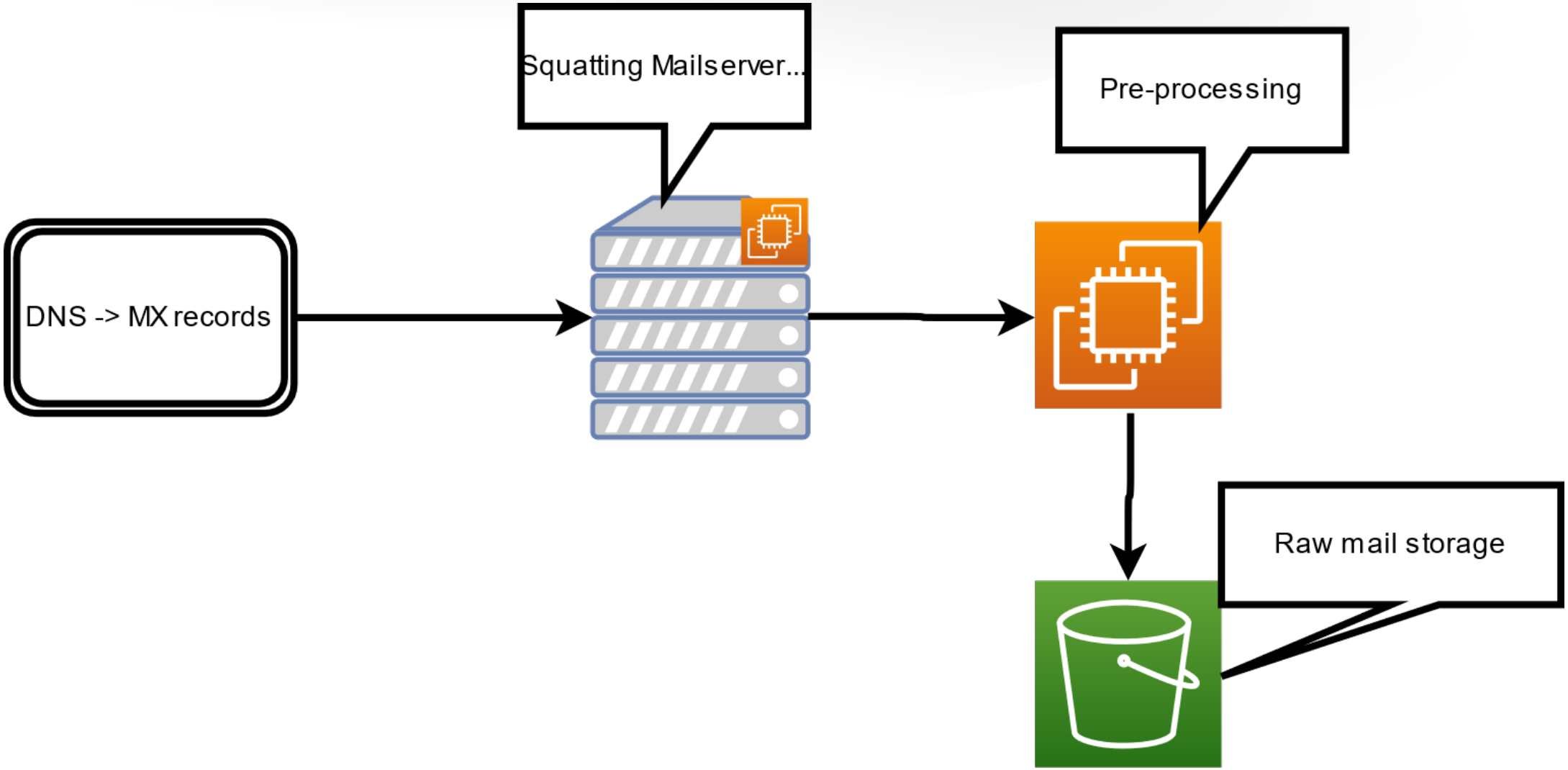
# The Target

- Multinational Medical service provider
  - Hospital services
  - Pharmaceutical services
  - Doctor and specialist services
  - 5,000+ employees
- Interactions
  - Employees
  - Patient (Medical, financial)
  - Suppliers (Services, Productions and infrastructure)
  - Government (Healthcare, financial and law enforcement)
- Highly sensitive data

# Choosing our domain

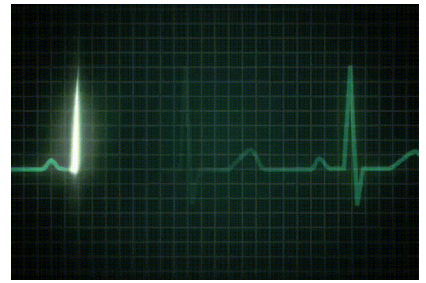
- Breach data as “validation source”
  - There is lots of it, and mostly free
  - Typo’s in breach data is usually caused by people mistyping their own email address
  - Typo domains with multiple occurrences in breach data is typically a good indication
- Found a target domain with multiple unique accounts (Lots of employees making the same mistake)

# The Setup

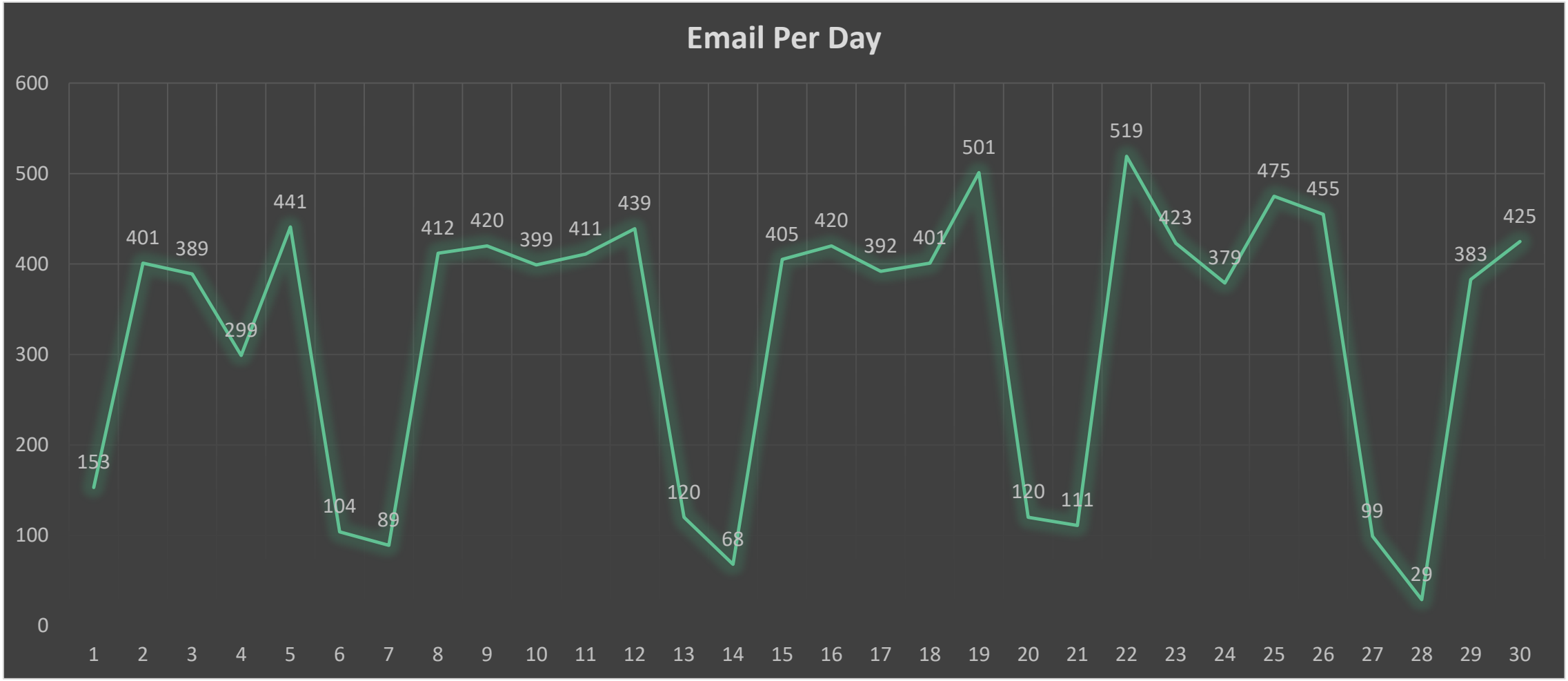

Squatting Mailserver...
Pre-processing
DNS -> MX records
Raw mail storage

# General Statistics

- First email received within 2 min
- 10,000+ emails received during 30 day period
- ~2,600 legitimate file attachments (disregarded images from mail signatures, etc.) of these 850 were classed as business related documents
- 12.6% of emails received were from target organization internally

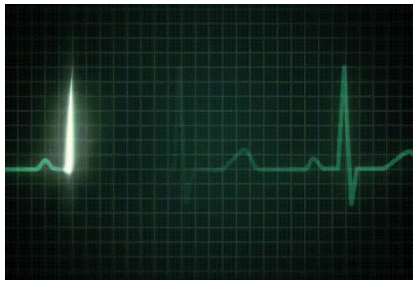


# General Statistics

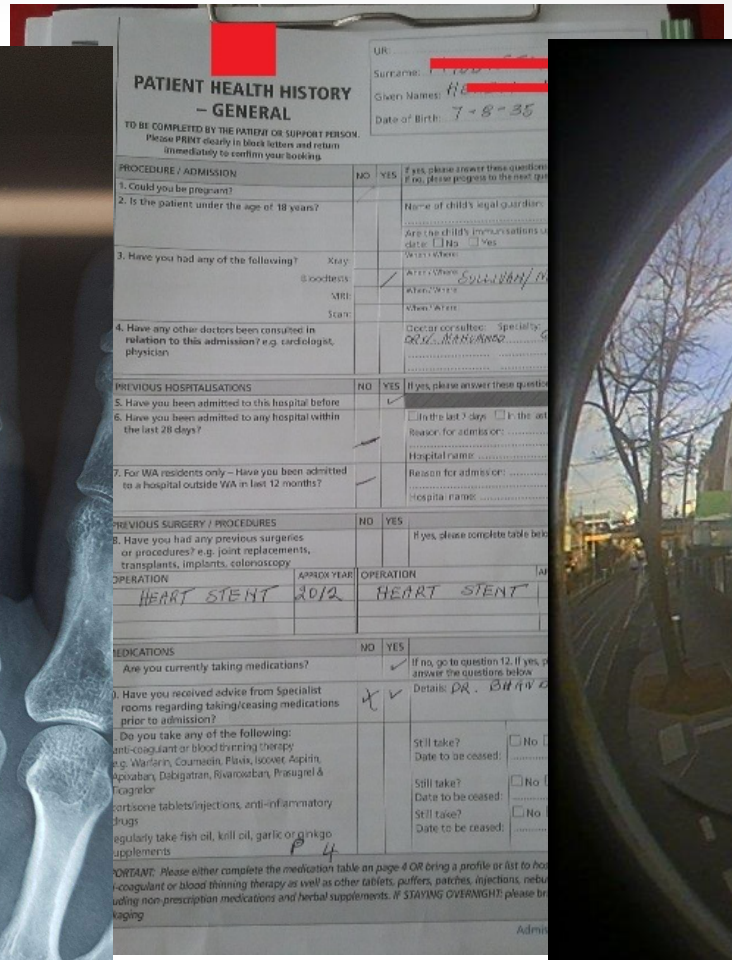


# General Statistics

- First email received within 2 min
- 10,000+ emails received during 30 day period
- ~2,600 legitimate file attachments (disregarded images from mail signatures etc) of these 850 was classed as business related documents
- 12.6% of emails received was from target organization internally



# Loot



PATIENT HEALTH HISTORY
– GENERAL

TO BE COMPLETED BY THE PATIENT OR SUPPORT PERSON.
Please PRINT clearly in black letters and return immediately to confirm your booking.

UR:
Surname:
Given Names:
Date of Birth: 7-8-35

| PROCEDURE / ADMISSION | NO | YES |
|---|---|---|
| 1. Could you be pregnant? | | |
| 2. Is the patient under the age of 18 years? | | |
| 3. Have you had any of the following? X-ray | | |
| Bloodtests | | ✓ |
| MRI | | |
| Scan | | |
| 4. Have any other doctors been consulted in relation to this admission? e.g. cardiologist, physician | | |

| PREVIOUS HOSPITALISATIONS | NO | YES |
|---|---|---|
| 5. Have you been admitted to this hospital before | | ✓ |
| 6. Have you been admitted to any hospital within the last 28 days? | ✓ | |
| 7. For WA residents only – Have you been admitted to a hospital outside WA in last 12 months? | ✓ | |

| PREVIOUS SURGERY / PROCEDURES | NO | YES |
|---|---|---|
| 8. Have you had any previous surgeries or procedures? e.g. joint replacements, transplants, implants, colonoscopy | | |

| OPERATION | APPROX YEAR | OPERATION |
|---|---|---|
| HEART STENT | 2012 | HEART STENT |

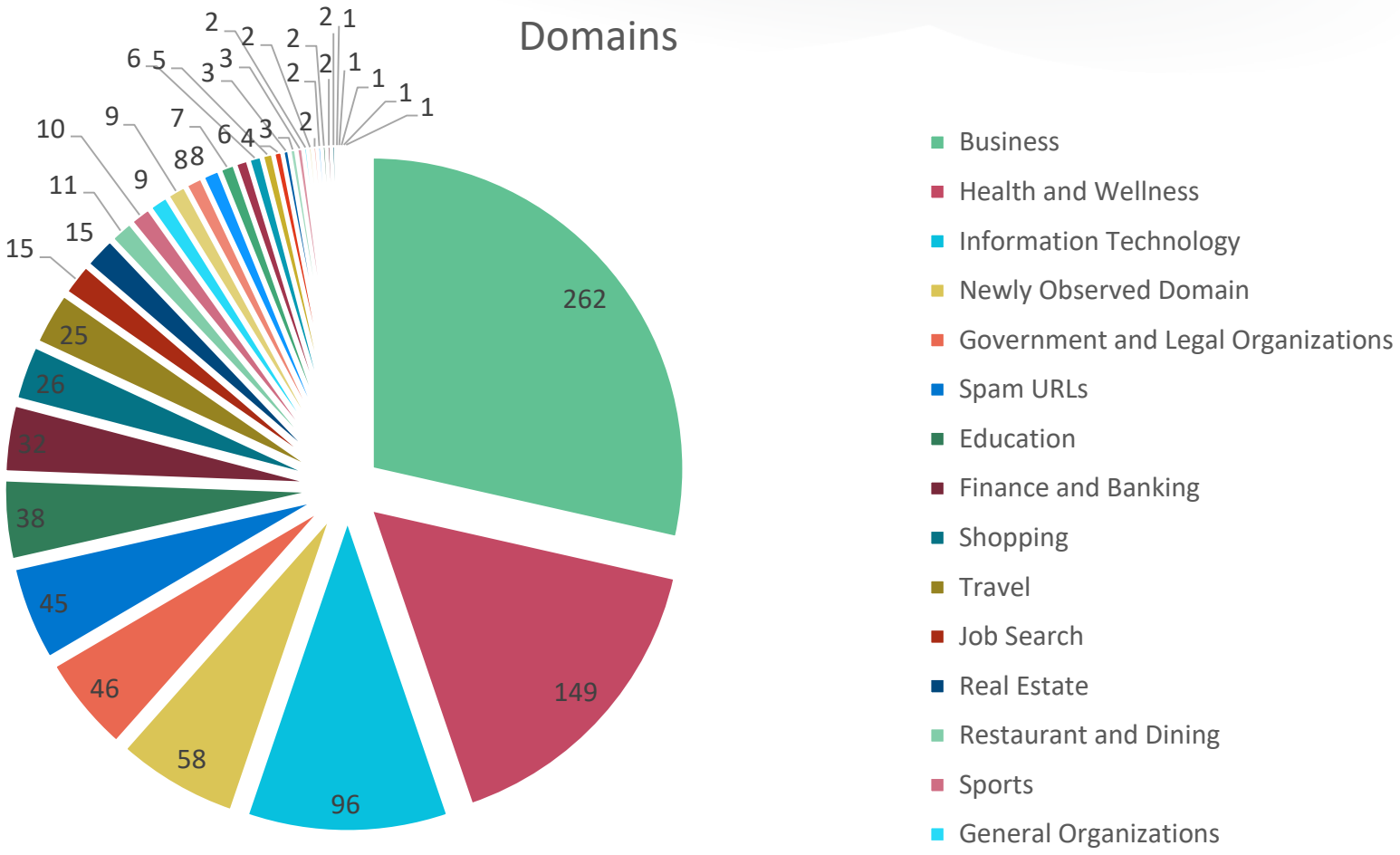
| MEDICATIONS | NO | YES |
|---|---|---|
| Are you currently taking medications? | | ✓ |
| 10. Have you received advice from Specialist rooms regarding taking/ceasing medications prior to admission? | ✓ | |

11. Do you take any of the following:
anti-coagulant or blood thinning therapy
e.g. Warfarin, Coumadin, Plavix, Iscover, Aspirin, Apixaban, Dabigatran, Rivaroxaban, Prasugrel & Ticagrelor
cortisone tablets/injections, anti-inflammatory drugs
regularly take fish oil, krill oil, garlic or ginkgo supplements

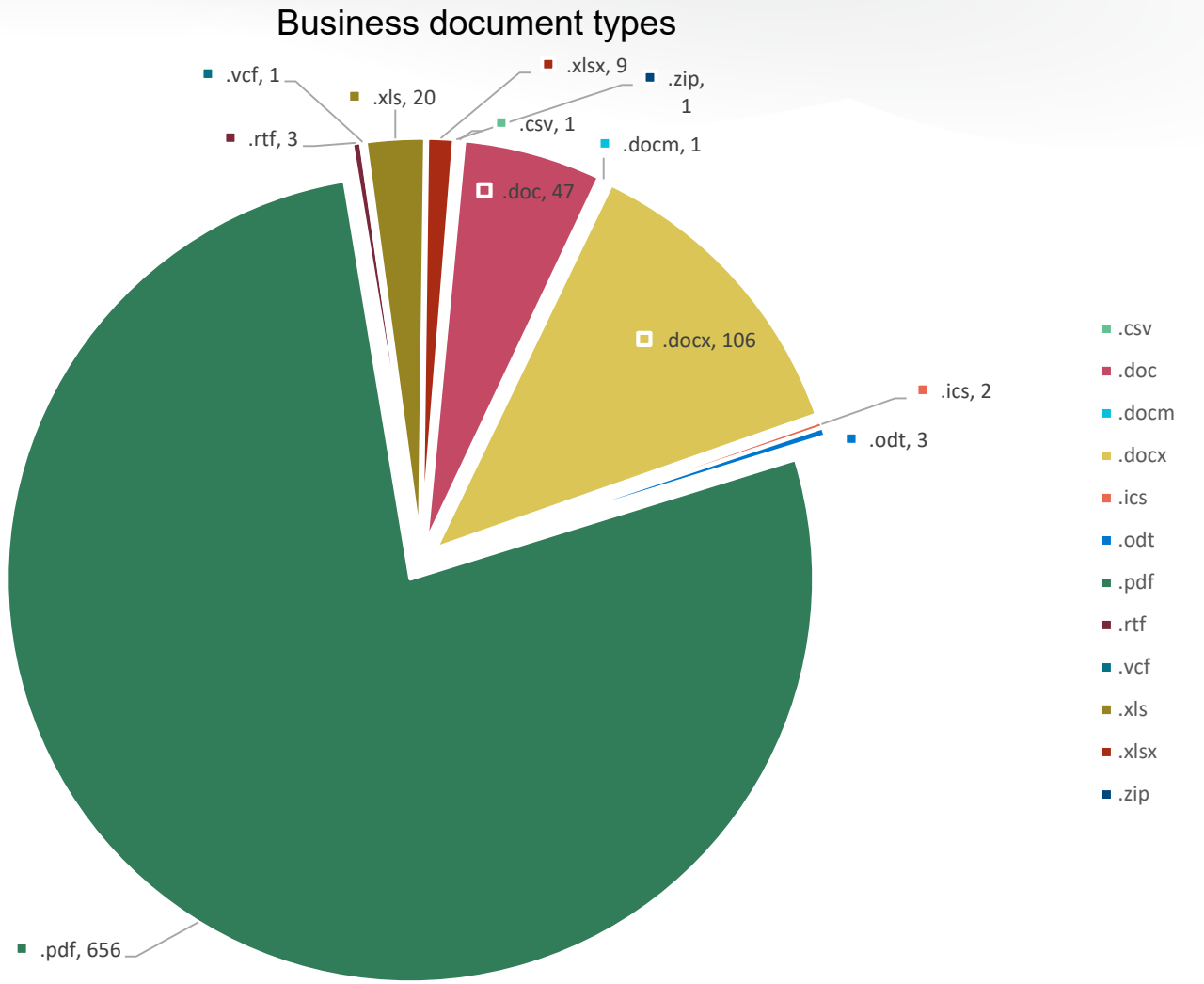
P 4

IMPORTANT: Please either complete the medication table on page 4 OR bring a profile or list to ho
anti-coagulant or blood thinning therapy as well as other tablets, puffers, patches, injections, nebu
including non-prescription medications and herbal supplements. IF STAYING OVERNIGHT: please br
Imaging

# Who Were Sending The Emails



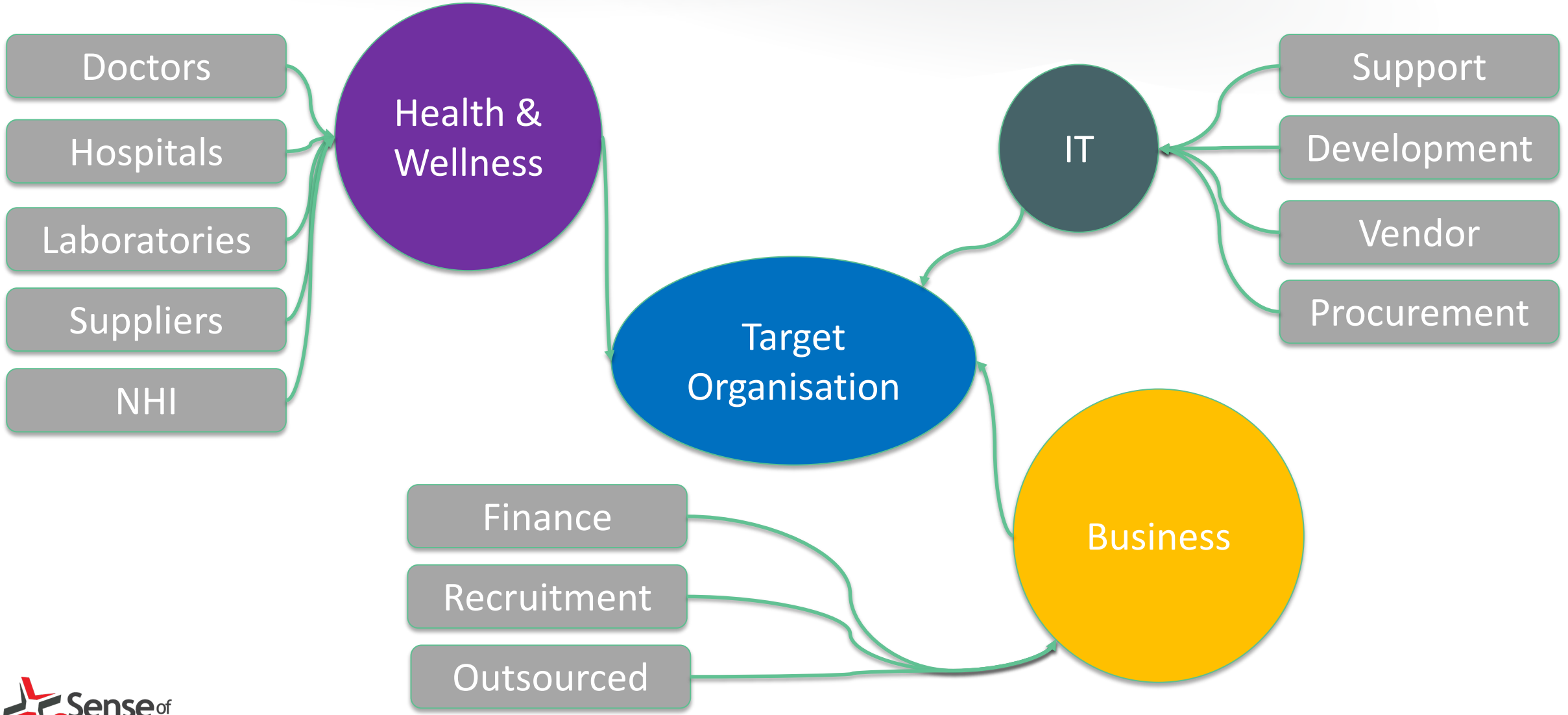
# Attachment Breakdown



# Leaky MFPs

| Subject |
| --- |
| Scanned from a Xerox Multifunction Printer |
| Scan from a Samsung MFP |
| Scanned from a Xerox Multifunction Printer |
| Scanned from a Xerox multifunction device |
| Scanned from a Xerox multifunction device |
| FW: Scan from a Xerox Phaser MFP |
| FW: Scan from a Xerox WorkCentre |
| FW: Scan from a Xerox WorkCentre |
| FW: Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| Scan from a Xerox WorkCentre |
| FW: Scanned from a Xerox Multifunction Printer |
| FW: Scan from a Xerox WorkCentre |
| Scan from a Xerox Phaser MFP |

# Supply Chain map



# Conversations – Information & Technology

# Conversations – Information & Technology

RSAConference2020

# Chapter 3: Execute plan A! …B…C

# Putting the Information to Work – Plan A

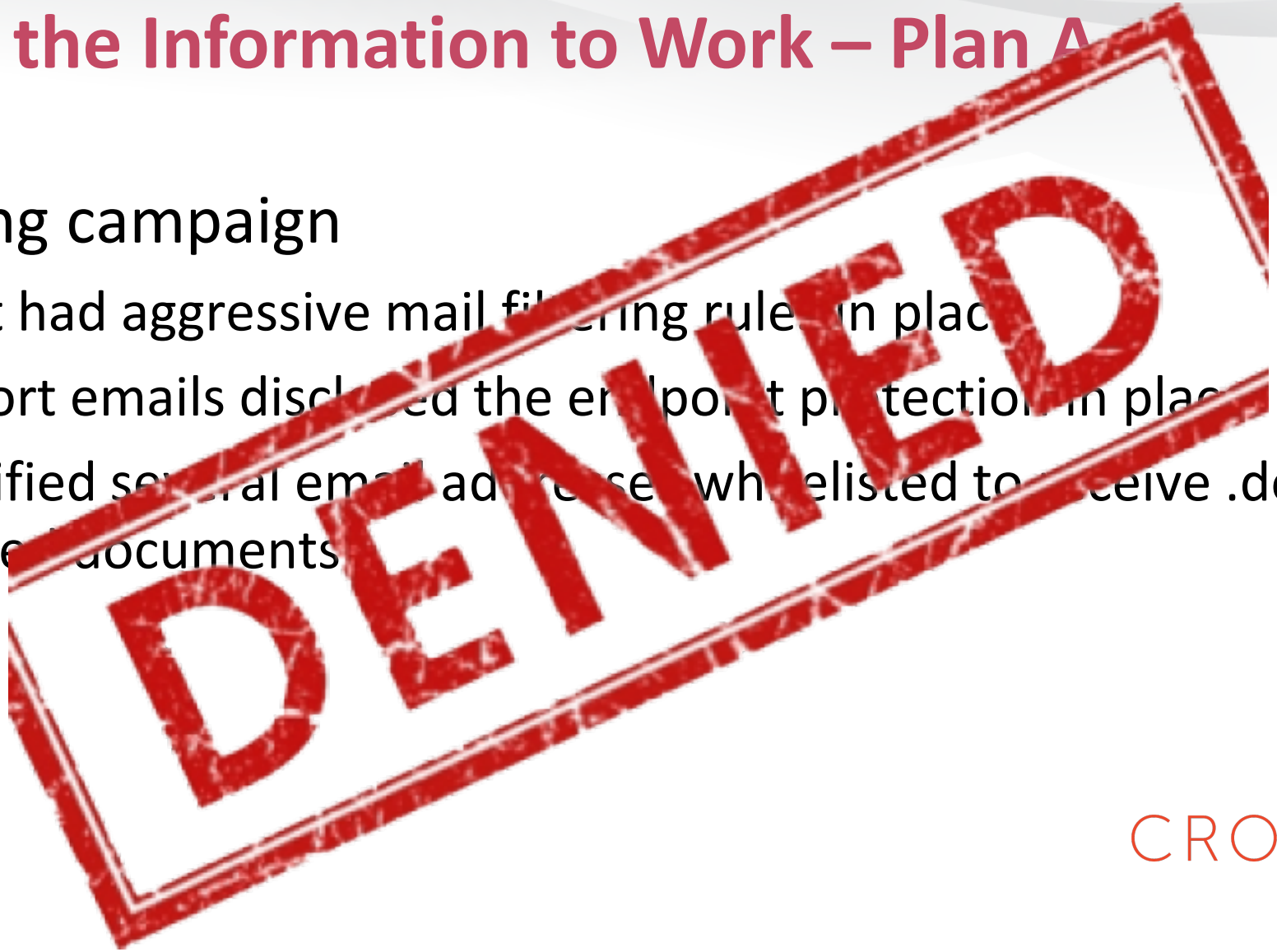
## The Phish…

- Phishing campaign
  - Client had aggressive mail filtering rules in place
  - Support emails disclosed the endpoint protection in place
  - Identified several email addresses whitelisted to receive .docm macro enabled documents

# Putting the Information to Work – Plan A

## The Phish…

- Phishing campaign
  - Client had aggressive mail filtering rules in place
  - Support emails disclosed the endpoint protection in place
  - Identified several email addresses whitelisted to receive .docm macro enabled documents




CROWDSTRIKE

Sense of Security
A CyberCX company

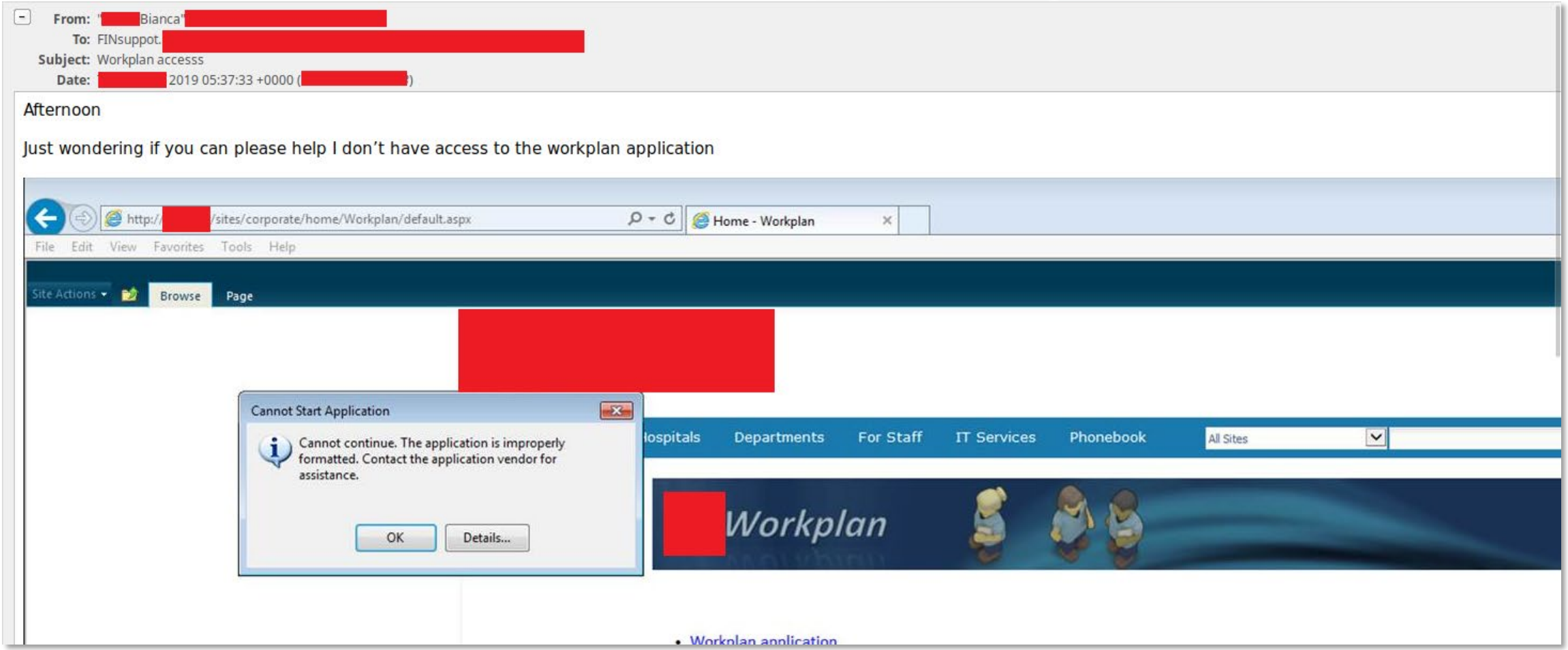
# Putting the Information to Work – Plan B

## Hello Bianca, this is Will from FINSupport…

- Telephone campaign (Vishing)
  - Zero success due to heightened client employee awareness
  - Using application support ticket as pretext for call
  - 100% success in convincing target that we are from IT ☺

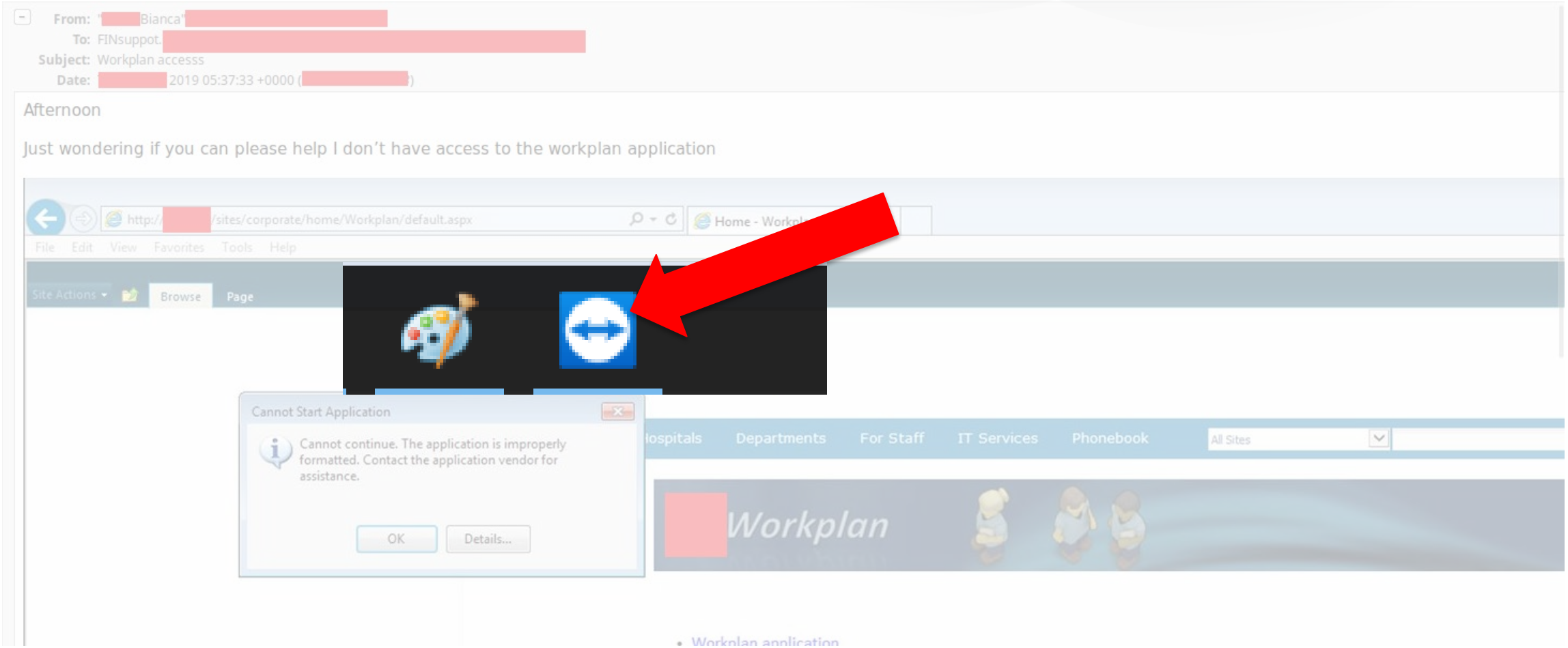
# Putting the Information to Work

## Hello Bianca, this is Will from FINSupport…



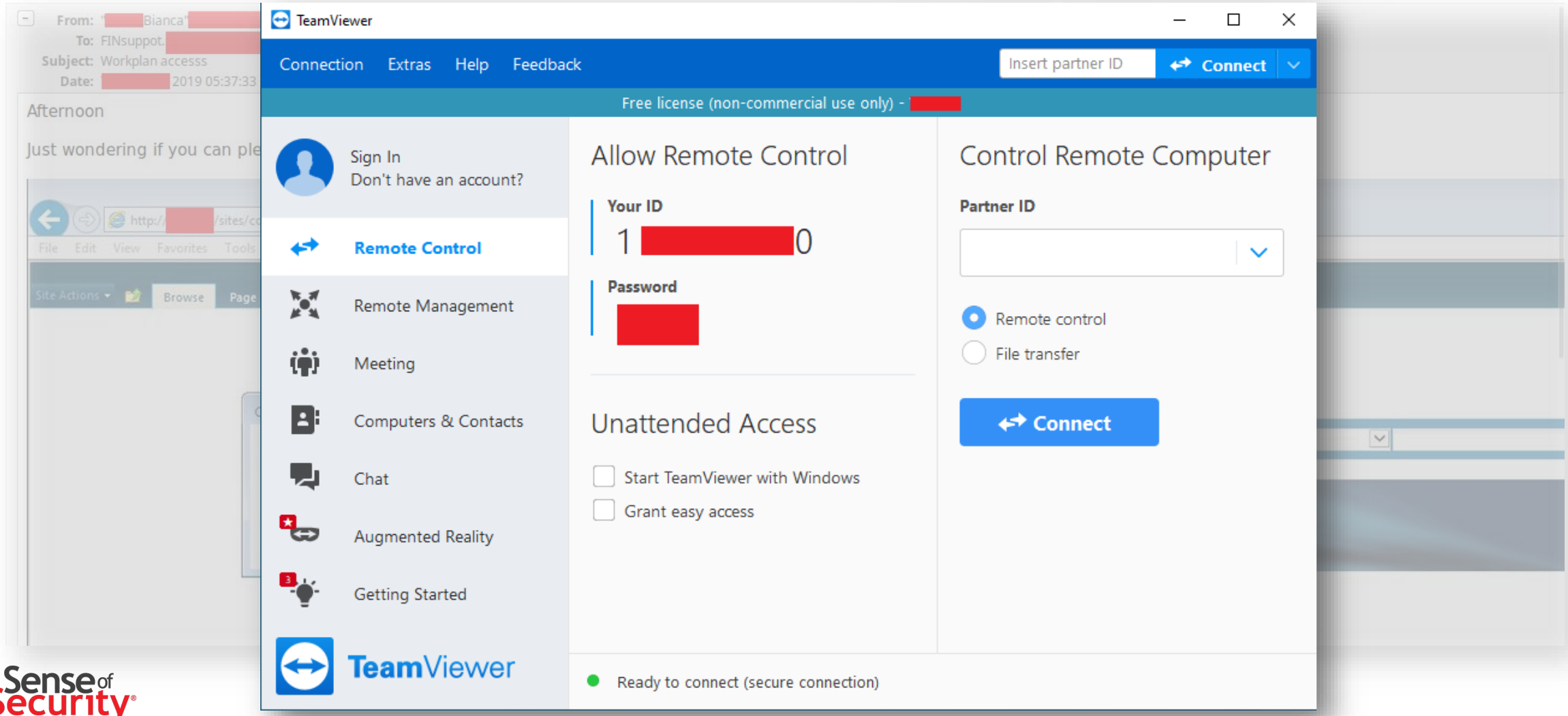
# Putting the Information to Work

## Hello Bianca, this is Will from FINSupport…



# Putting the Information to Work

## Hello Bianca, this is Will from FINSupport…



# Putting the Information to Work

## At the end of the rainbow

- Internal information
  - Received onboarding emails containing domain information from HR systems
  - Internal Risk management system password reset / registration emails
  - Sensitive business and internal documents from multifunction office devices

RSAConference2020

# Defensive measures

# Apply

- Proactive actions
  - Up to date domain inventory
  - Register trademarks
  - Response procedures / takedown playbooks
  - Employee education
- Reactive actions
  - Monitor internet sources for potentially risky domain registrations
  - Identify typo domains within your mail server logs
  - Take control (and keep control) of the riskiest domains

# Questions


A CyberCX company


Cyber Security + Customer Experience

Jeremy du Bruyn
jeremyd@senseofsecurity.com.au

Willem Mouton
willemm@senseofsecurity.com.au