



proofpoint®



Healthcare Threat Intel Briefing

Ryan Witt - Chair, Proofpoint Healthcare Customer Advisory Board
Resident CISO, Healthcare

proofpoint® Healthcare Overview

The leader in protecting people from advanced threats and compliance risk

Magic Quadrant leadership across:



Secure Email Gateway

Leader for 7 consecutive years



Security Awareness Training

Leader for 6 consecutive years



Information Archiving

Leader for 7 consecutive years



Cloud Access Security Broker

Leading Visionary

Enhancing knowledge of HC security challenges



HIMSS™

CHIME

AEHIS

Association for Executives in Healthcare Information Security



H-ISAC™

HEALTH - ISAC

proofpoint®

Healthcare Advisory Board

Trusted protection partner for health institutions



80% of top 20 hospitals

50% of top 10 children's hospitals

BECKER'S
HOSPITAL REVIEW

70% of 10 largest health systems

60% of top 30 not for profits

FORTUNE
100

74% of HC accounts in F100

BlueCross BlueShield

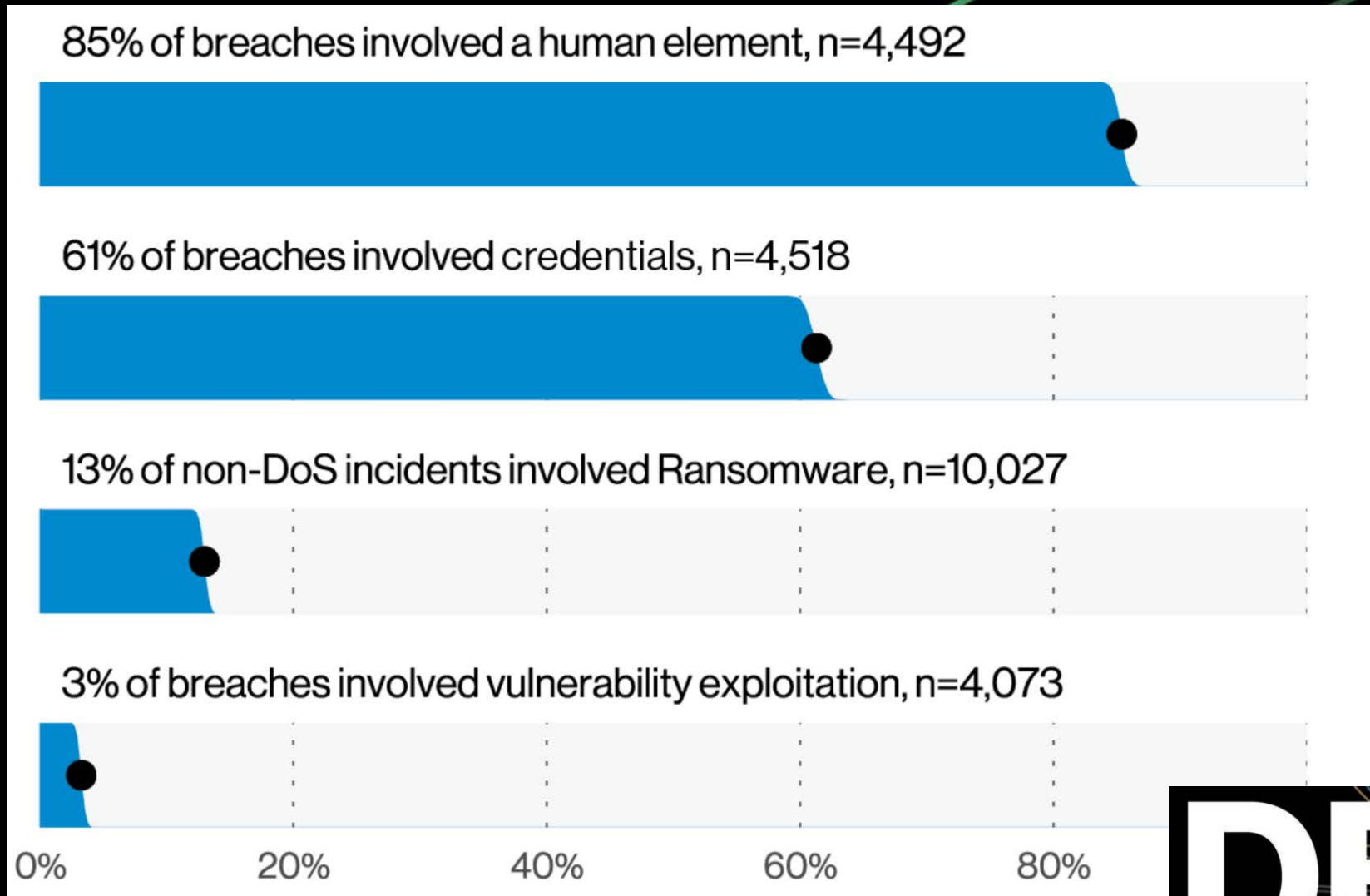
70% of the "Blues"

PharmExec

60% twenty largest pharma orgs



Cybersecurity Current State

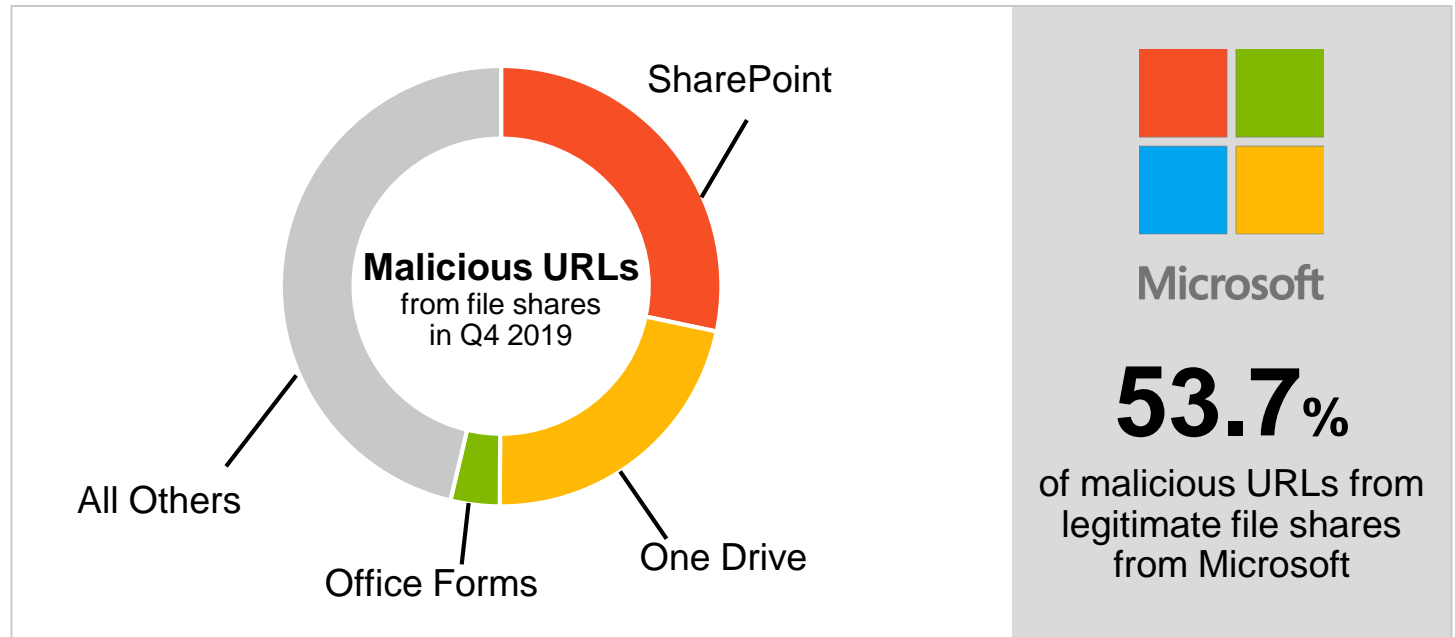


DBIR

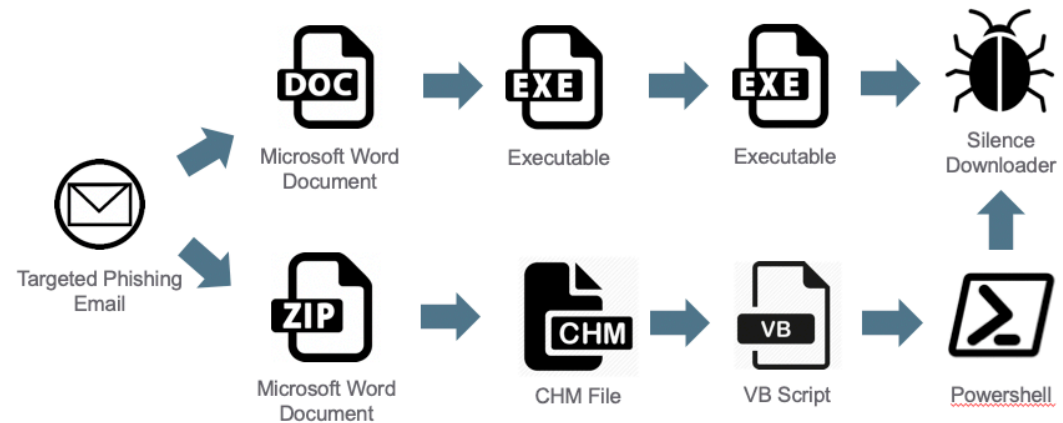
2021 Data Breach Investigations Report

Modern Threat Landscape

▶ More complex multi-stage threats



Attacker Innovation: RYUK Infection Chain

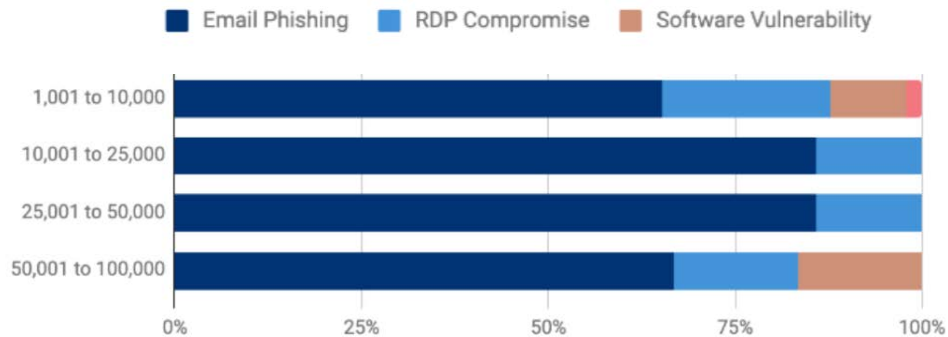


Beyond Data Breach: Top Risks Facing Enterprises

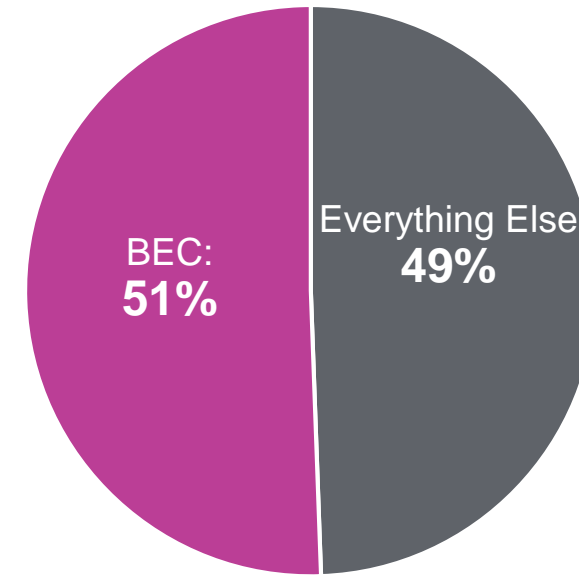
Ransomware:
90% successful attacks via email

BEC: Larger losses than all other threats *combined*

Attack Vector by Company Size



Source: Coveware Q4'20 Ransomware Report



Source: FBI / IC3

Top enterprise risks are people centric

Work From Anywhere Accelerates Risks

Many threats live within O365



59,809,708

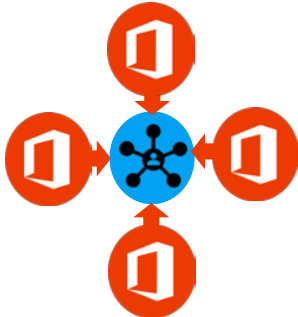
malicious messages from Microsoft in 2020 from

2,510,154

compromised accounts

Source: Proofpoint threat data

Compromised accounts fuel the entire threat landscape



98%

of Proofpoint customers attacked by a supplier/vendor

Source: Proofpoint research

Changing nature of work creates perfect storm for insider risk



31%

increase in insider threat incidents

\$11.45M

average incident loss

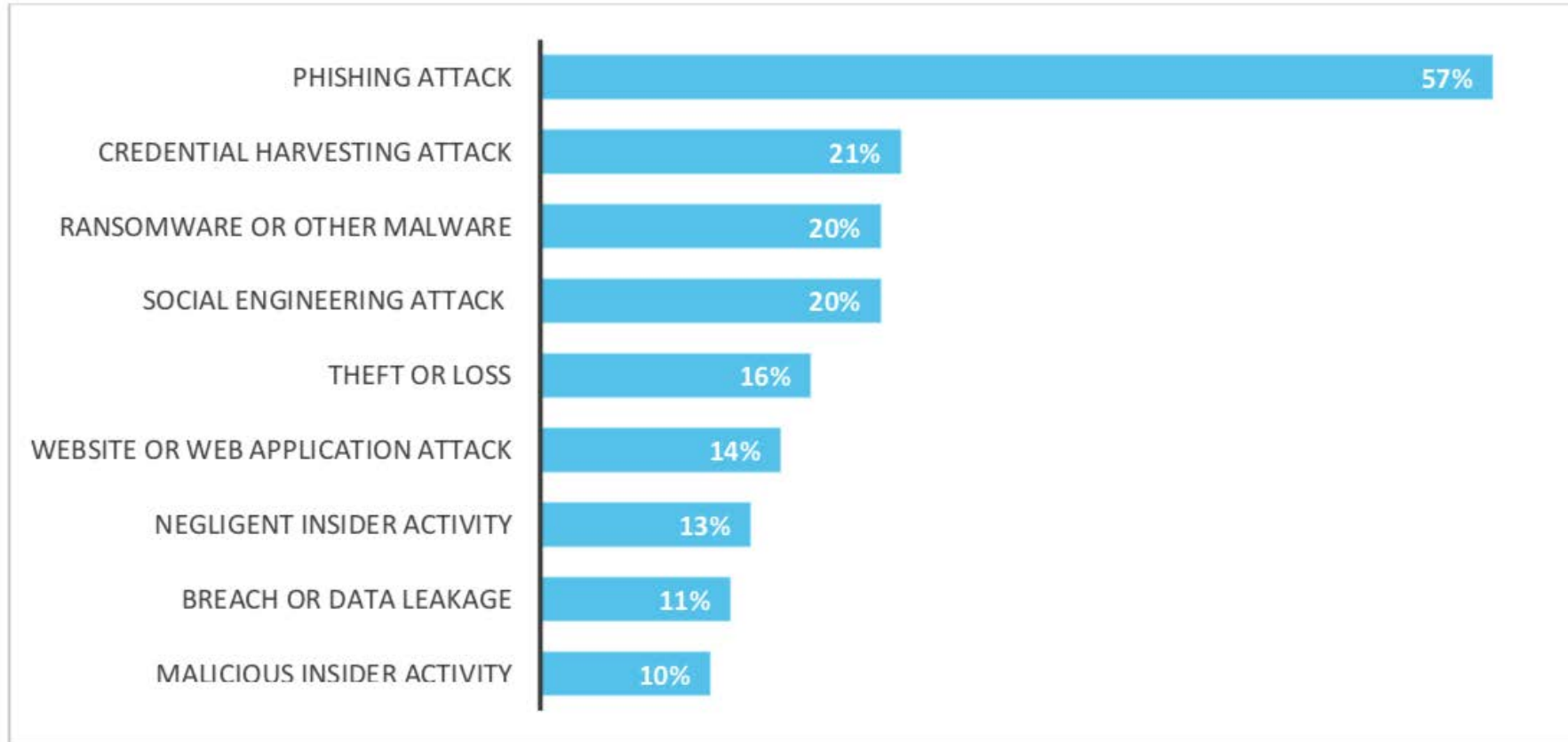
Source: Ponemon Institute, 2020 Cost of Insider Threats Global Study



Cybersecurity Current State – Healthcare

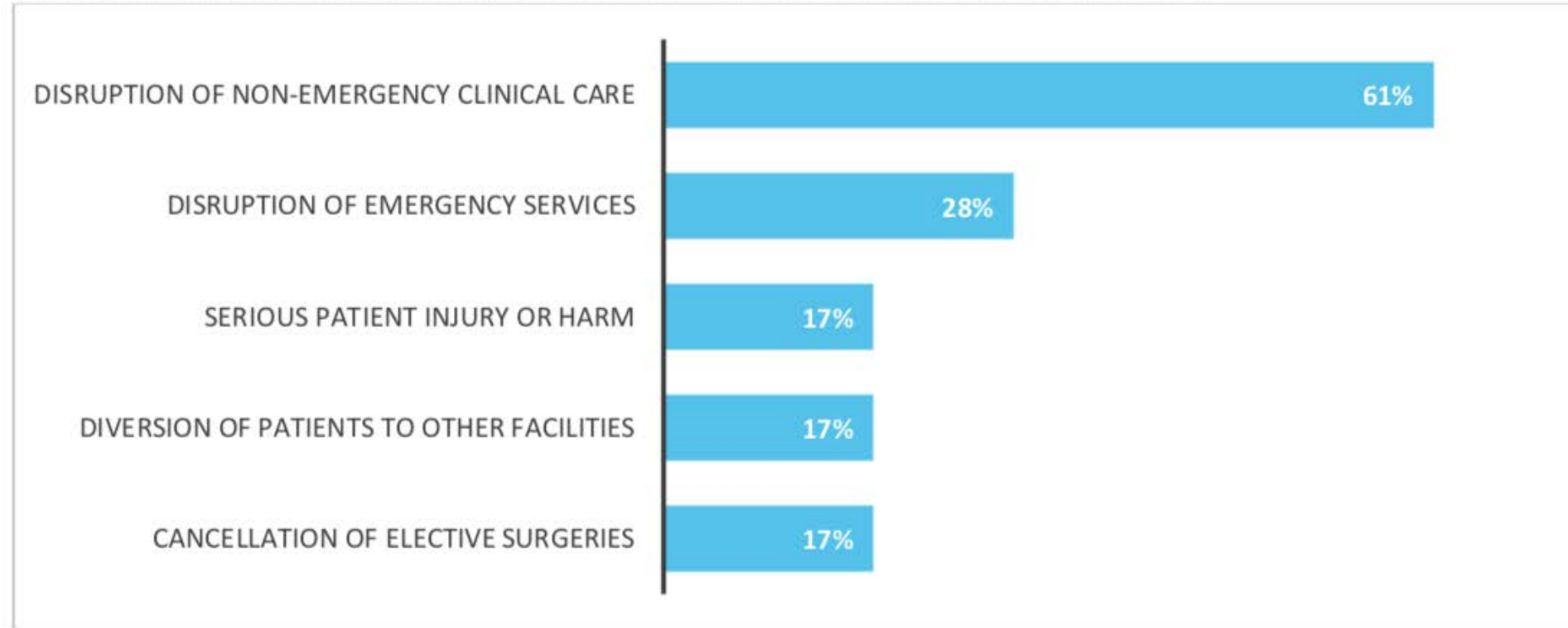
2020 Is About People Being Attacked...

Figure 1: Type of Significant Security Incident Experienced in the Past Twelve Months



...And Impacting Patient Safety

Figure 3: Significant Security Incidents – Types of Patient Safety Issues



...And the Initial Point of Compromise

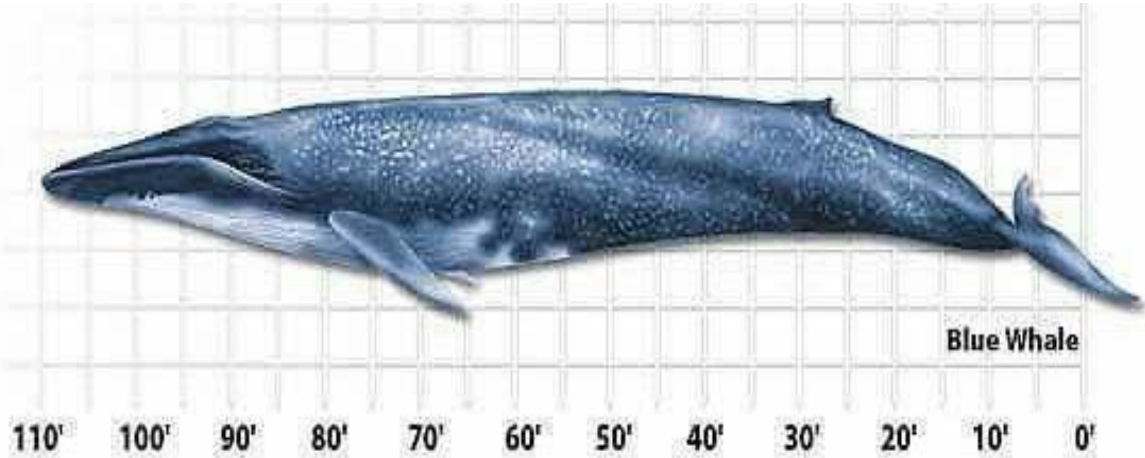
89% Via Email



Email Fraud is a Pervasive Threat

Supplier Fraud Accounts for Healthcare Largest Losses

Supplier Fraud



Blue Whale

Other BEC variants



Killer Whale (Orca)

Average healthcare organization received



200K emails from over

10K different domains

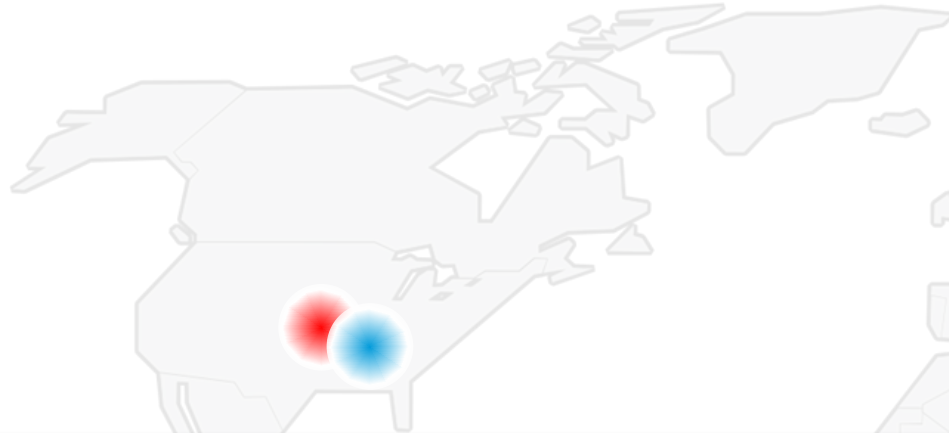
98% received an email-based threat



97%

of monitored healthcare organizations have received a threat from a supplier domain via impersonation or BEC

Healthcare Contractor



Location: USA
Date: January 12, 2021
Target: healthcare contractor
Supplier: Bob's Plumbers
Objective: steal money
Severity: **modest**

From: Bob@BobsPlumbers.com
To: Accounts Payable
Subject: Invoice 1234, Inc/ACH Payment

Hi All,

Sorry for the late response. I have been busy on the site.

I understand you do not ACH payments. Unfortunately, due to Covid-19 restrictions we cannot cash checks right now. Can payment be remitted directly through wire transfer? We will be responsible for the wire fees. Kindly deduct the wire fees from the original invoice amount.

Please advise so I can email our wire instructions.

Bob

Bob@BobsPlumbers.com

TTPs: social engineering
Covid-19 excuse
fee waive "carrot"
lookalike domain

Medical Supplier

Location: Pennsylvania
Date: April 2021 indictment
Target: "A Pennsylvania University"
Supplier: medical supplies
Severity: **\$2,000,000**

FOR IMMEDIATE RELEASE

Tuesday, April 20, 2021

Powder Springs man indicted for laundering over two million dollars in proceeds from a Business Email Compromise scheme

ATLANTA - Denis Onderi Makori has been indicted on charges relating to a business email compromise (BEC) scheme targeting a Pennsylvania university and allegedly defrauding it out of more than \$2 million.

"Business email compromise schemes pose a severe risk of financial loss to public and private institutions alike," said Acting U.S. Attorney Kurt R. Erskine. "In this case, Makori allegedly helped orchestrate a scheme that caused a university to transfer unknowingly over \$2 million to bank accounts he controlled."

"BEC schemes like this alleged one are a big reason why the Georgia Cyber Fraud Task Force, comprised of federal, state and local agencies, was launched in February," said Chris Hacker, Special Agent in Charge of FBI Atlanta. "It takes a combination of education and our priority to investigate and prosecute these cases to make it a deterrent to those who contemplate committing these crimes."

According to Acting U.S. Attorney Erskine, the indictment, and other information presented in court: Various individuals allegedly engaged in a fraudulent BEC scheme to cause a university located in Pennsylvania to send payments totaling more than \$2 million via Automated Clearing House (ACH) to a bank account controlled by Makori, rather than to the intended beneficiary of such payments, a medical supply company based in Alpharetta, Georgia.

Case Study – Children’s Hospital

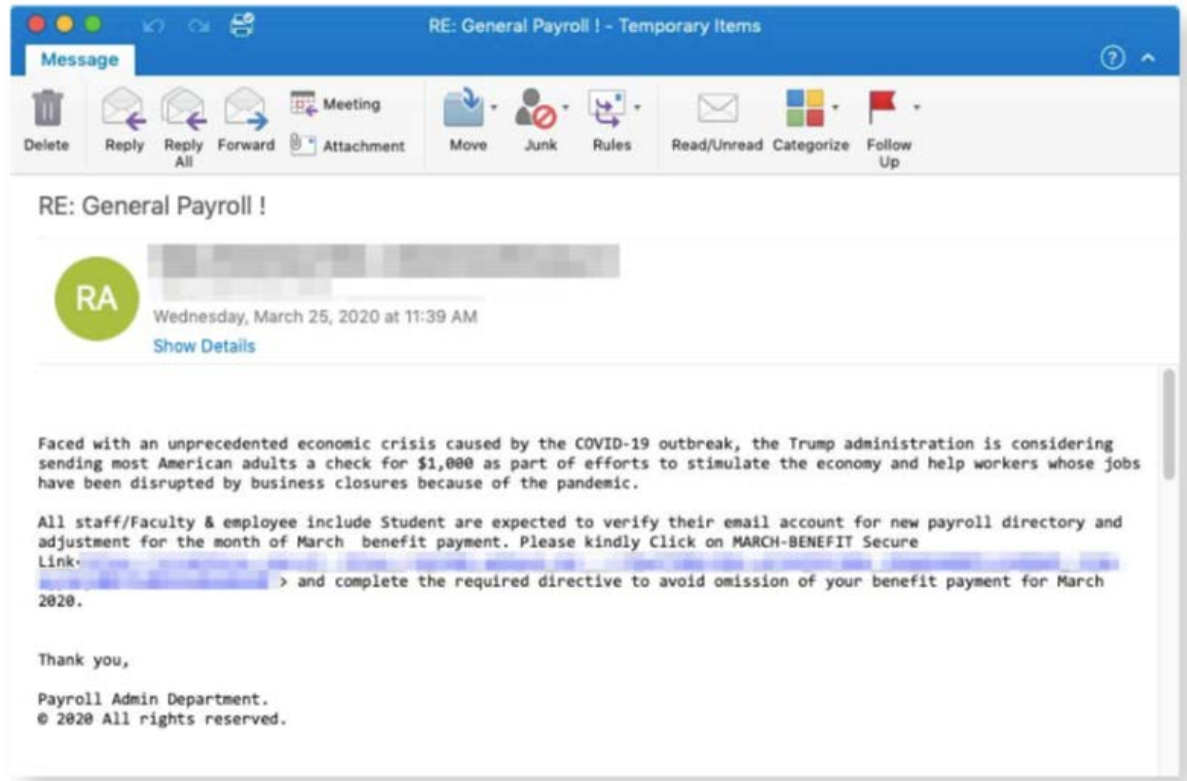


Figure 8. Cares Act payroll lure

- Lure – “Get Your Economic Stimulus Payment”
- Use of Social Engineering – referenced “US CARES Act”
- Target – pediatric care institutions
- Goal – PII / PHI, presumably for identify theft



Real World Threat Examples

Case Study – Targeted Credential Phishing (Provider)

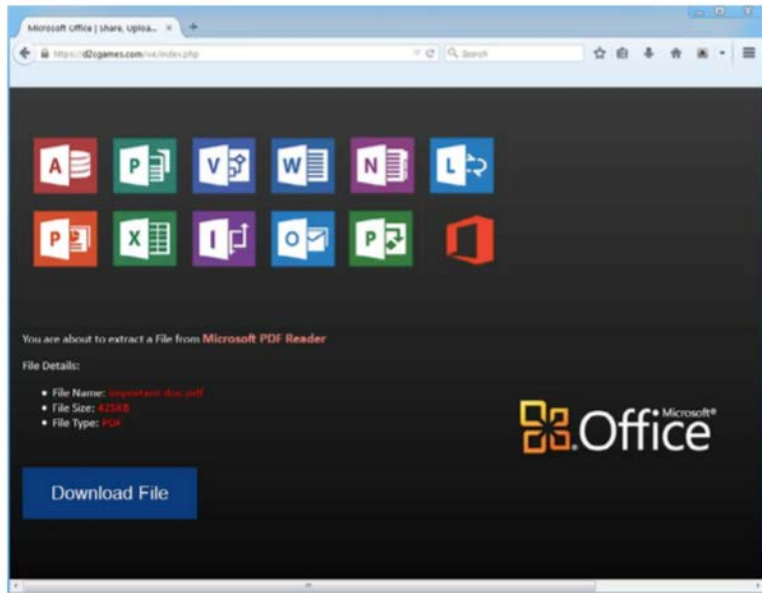


Figure 6. TA569 compromised website

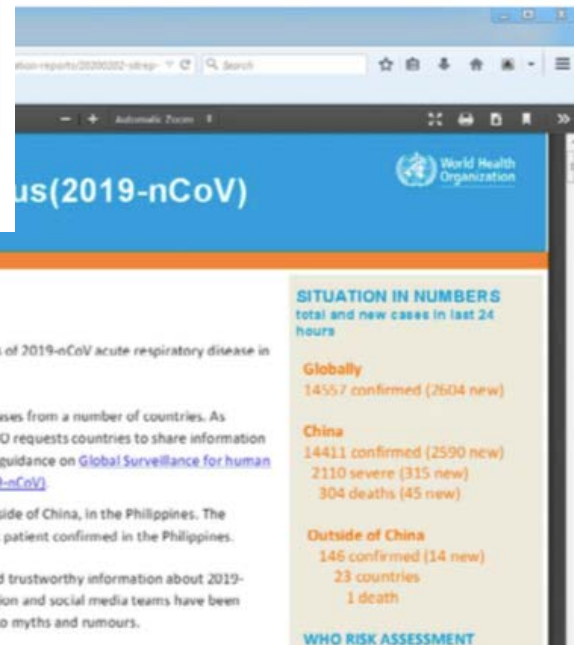
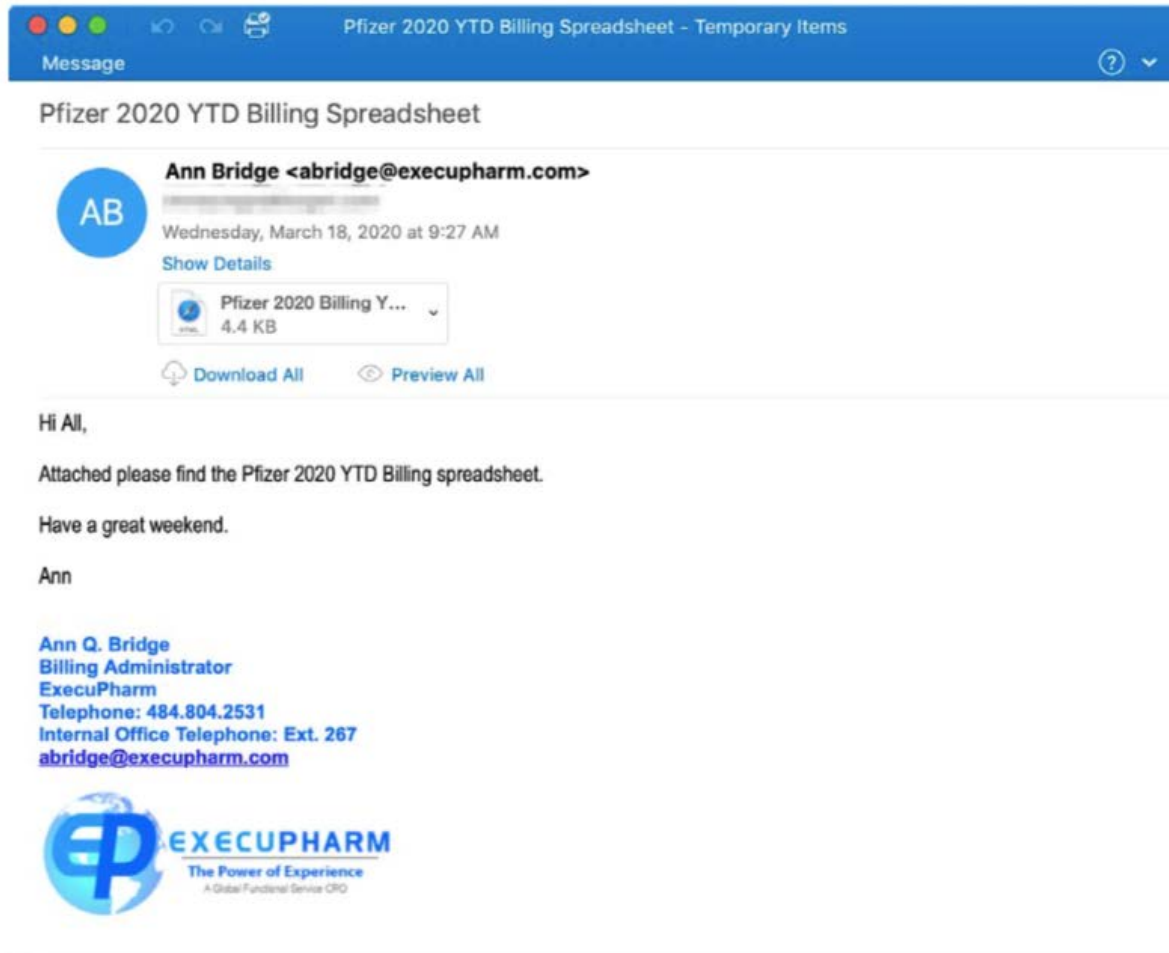


Figure 7. A legitimate benign COVID-19 WHO website

- Low volume, highly targeted
- Lure – Imposter email purporting to come from institution CEO re COVID travel restrictions
- Requested employees to download document from spoofed Microsoft website
- Once credentials provided, redirects to genuine WHO website to substantiate lure
- Goal – Credential Phishing

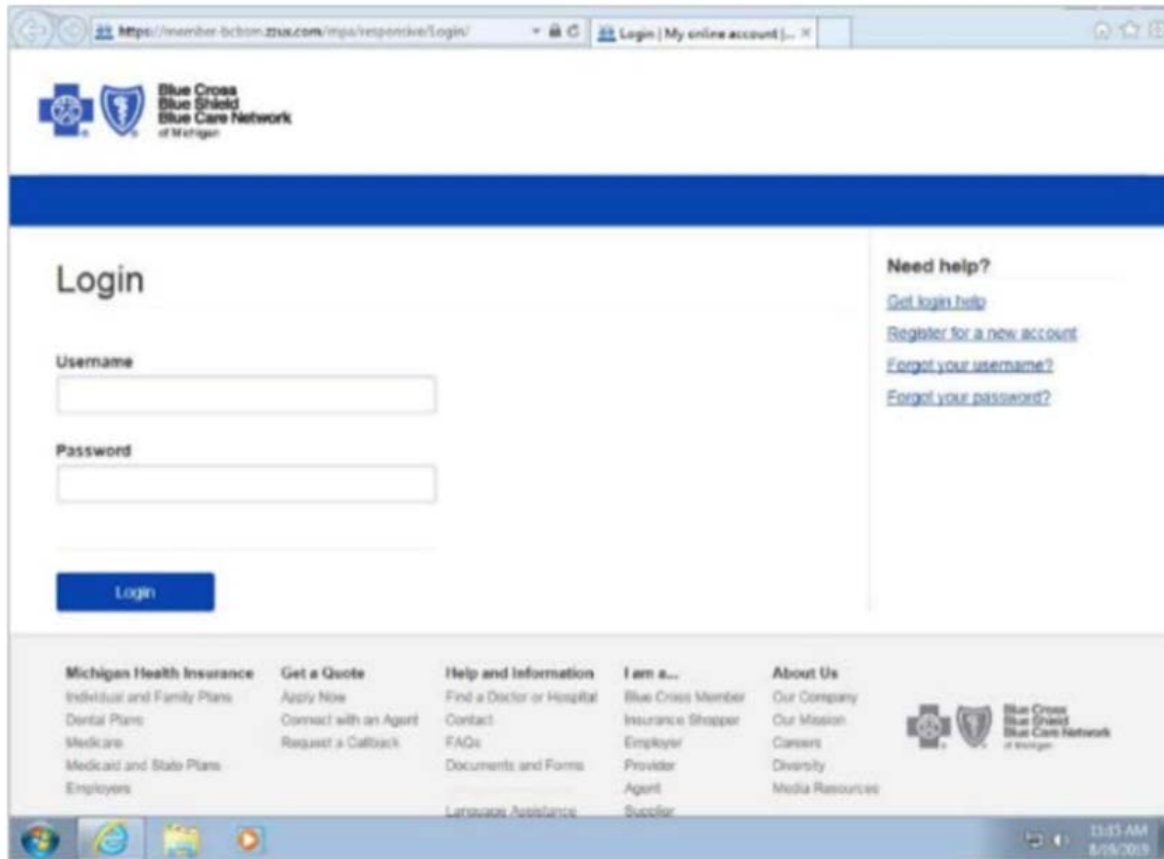
Case Study – Pharma Life Science



- From TA505, known for large scale crimeware campaigns
- Favored malware - SDBot RAT and Get2 Downloader
- Targeted pharma market (78% of 250K message campaign)
- Focused on COVID-19 clinical researchers

Figure 5. TA569 compromised website

Case Study – Health Insurers



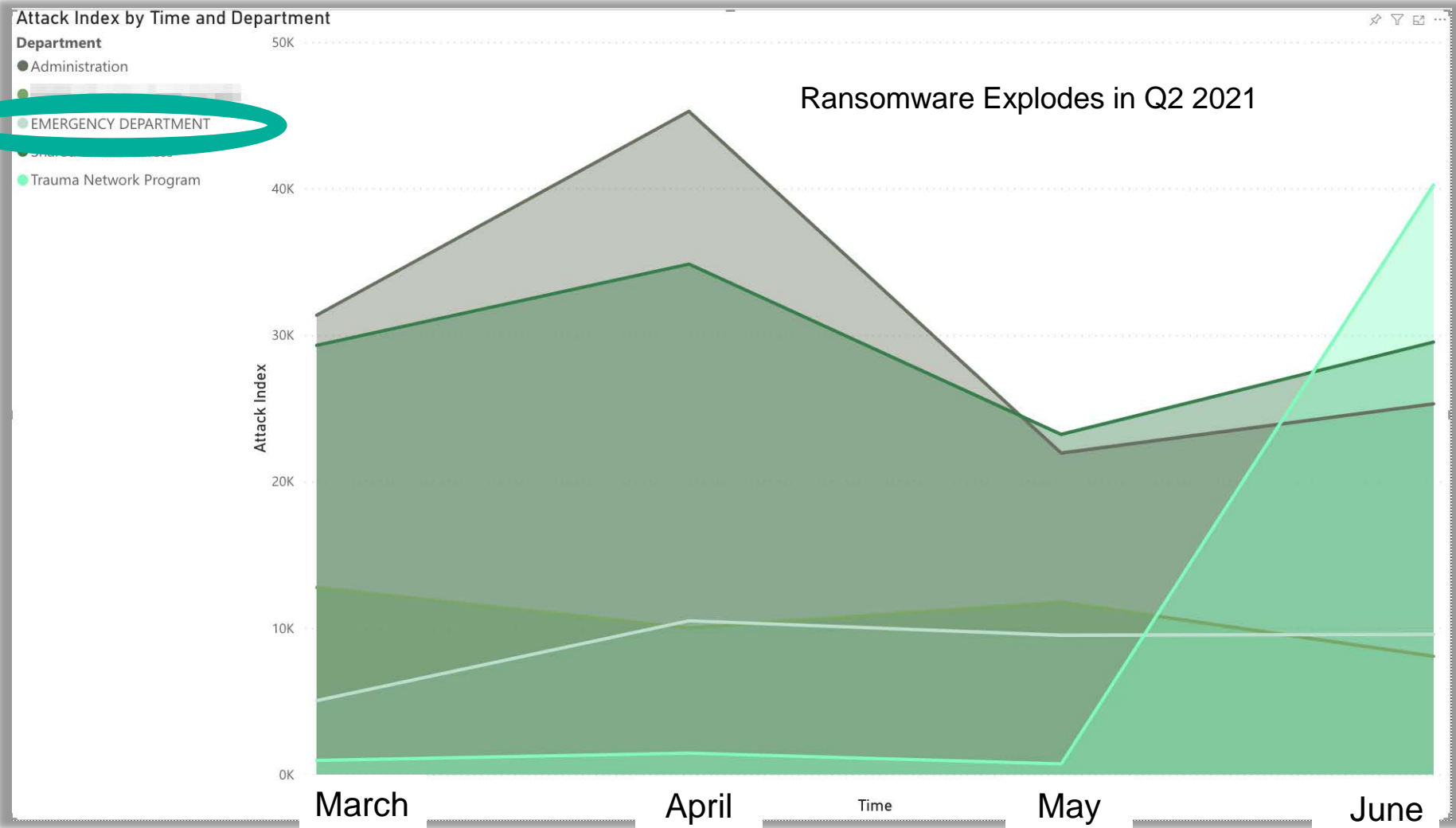
- Lure – “Updating Our Privacy Policy Settings”
- Email spoofed to make it look like it comes from “Blue Cross Blue Shield Association”
- Link to a cloned portal purporting to be from Blue Cross Blue Shield of Michigan
- Goal – credential harvesting

Figure 9. A cloned portal meant to mimic an Insurer

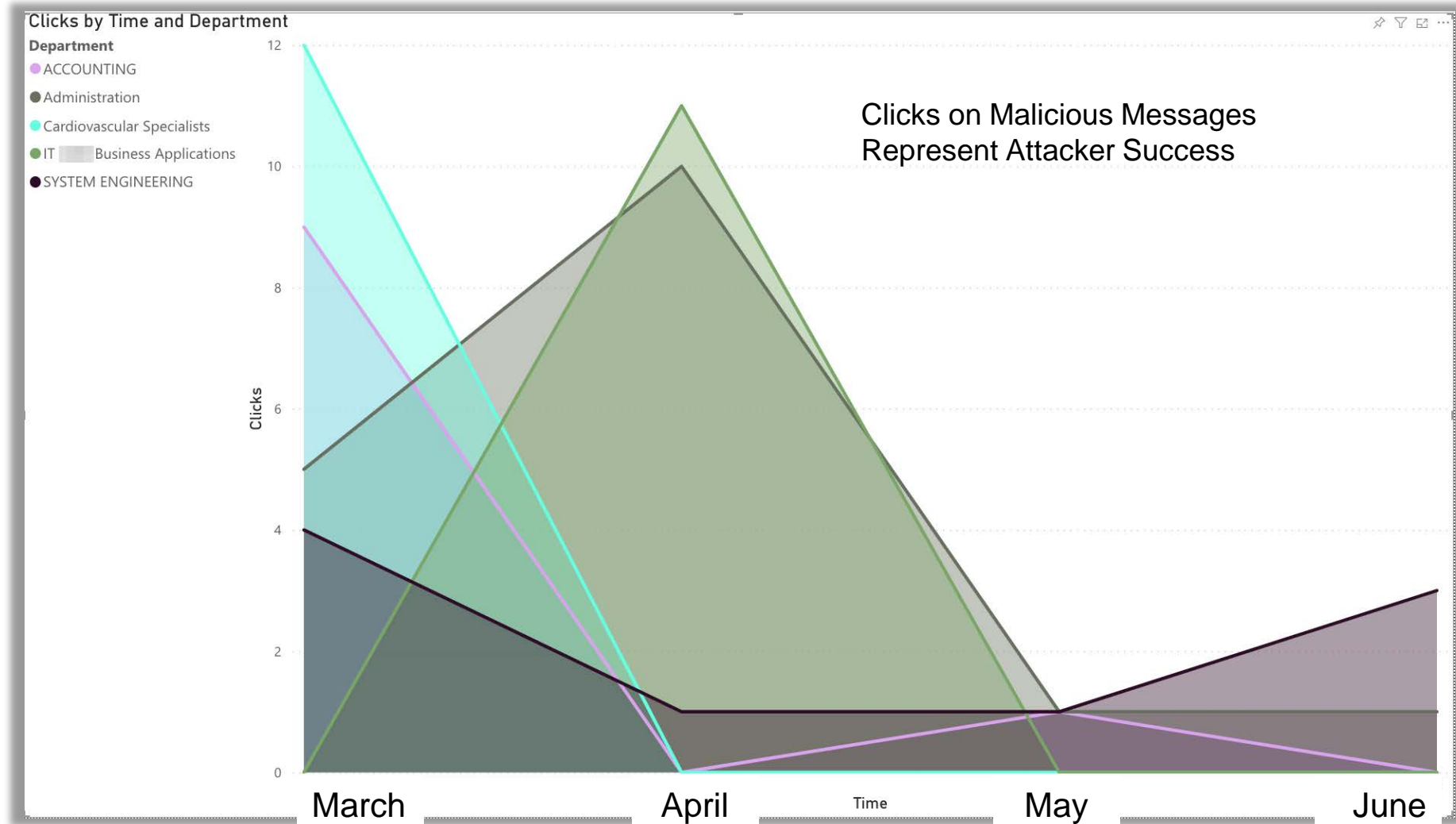


The Malware Elephant in the Room

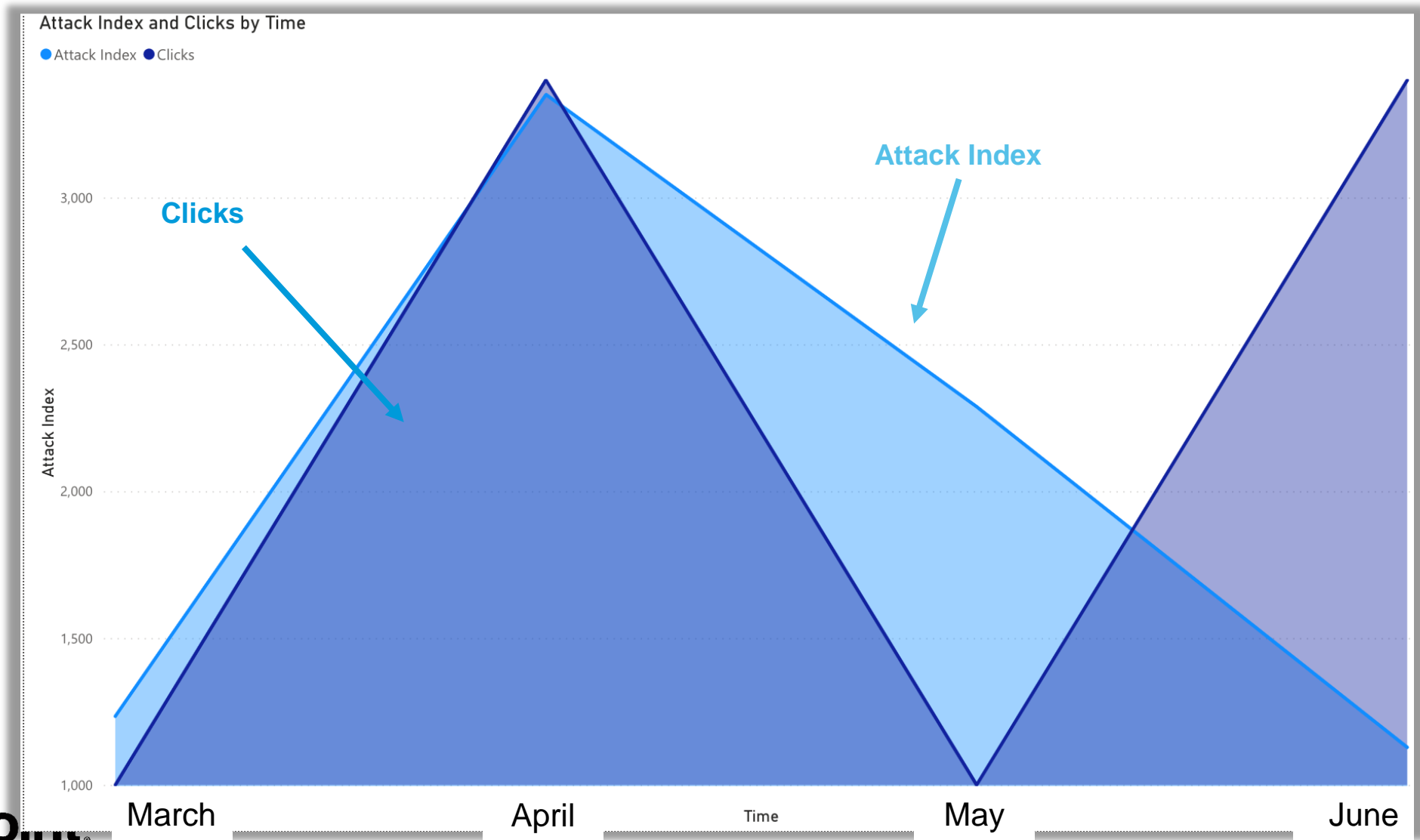
How Cyberattacks Become a Patient Safety Issue



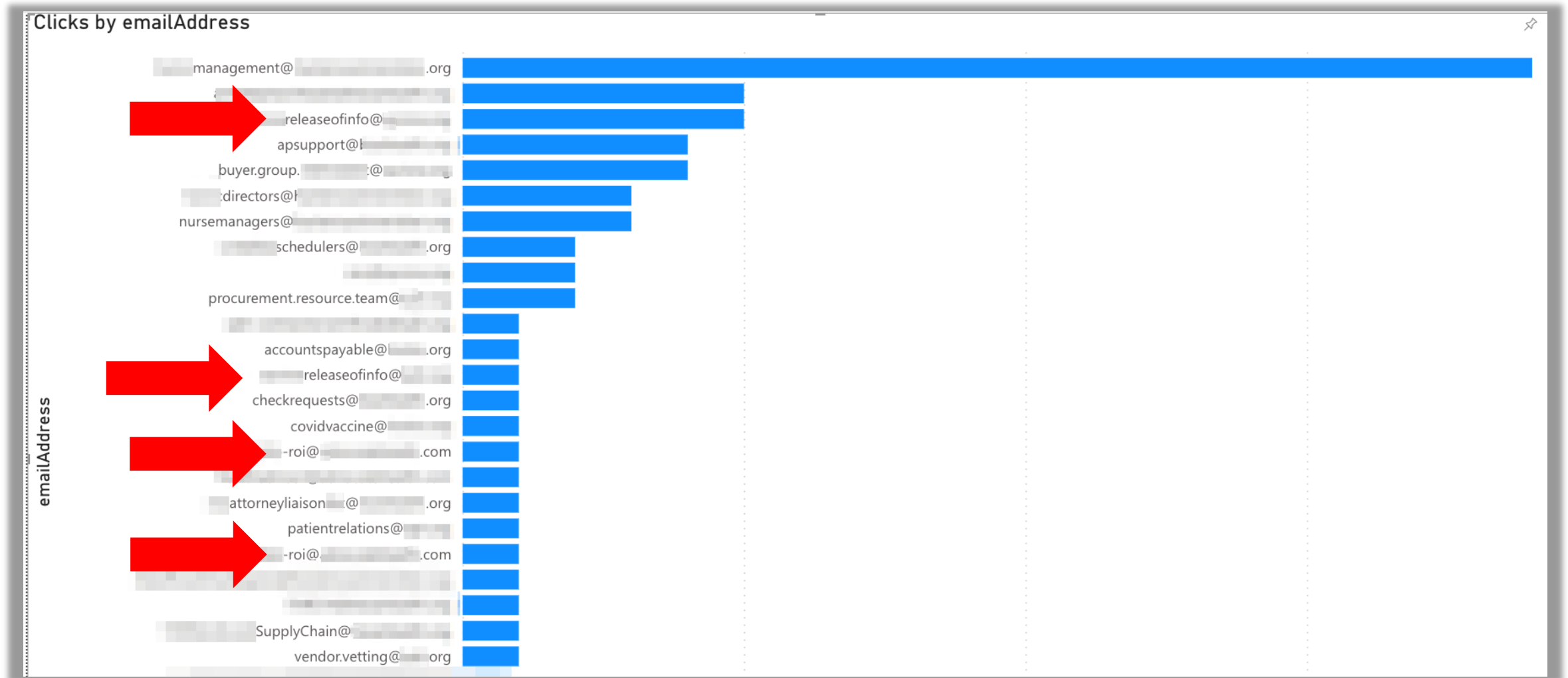
How Does Ransomware Enter Healthcare



Attackers Focus on Release of Information Department


















Who Are Ransomware Actors Targeting?



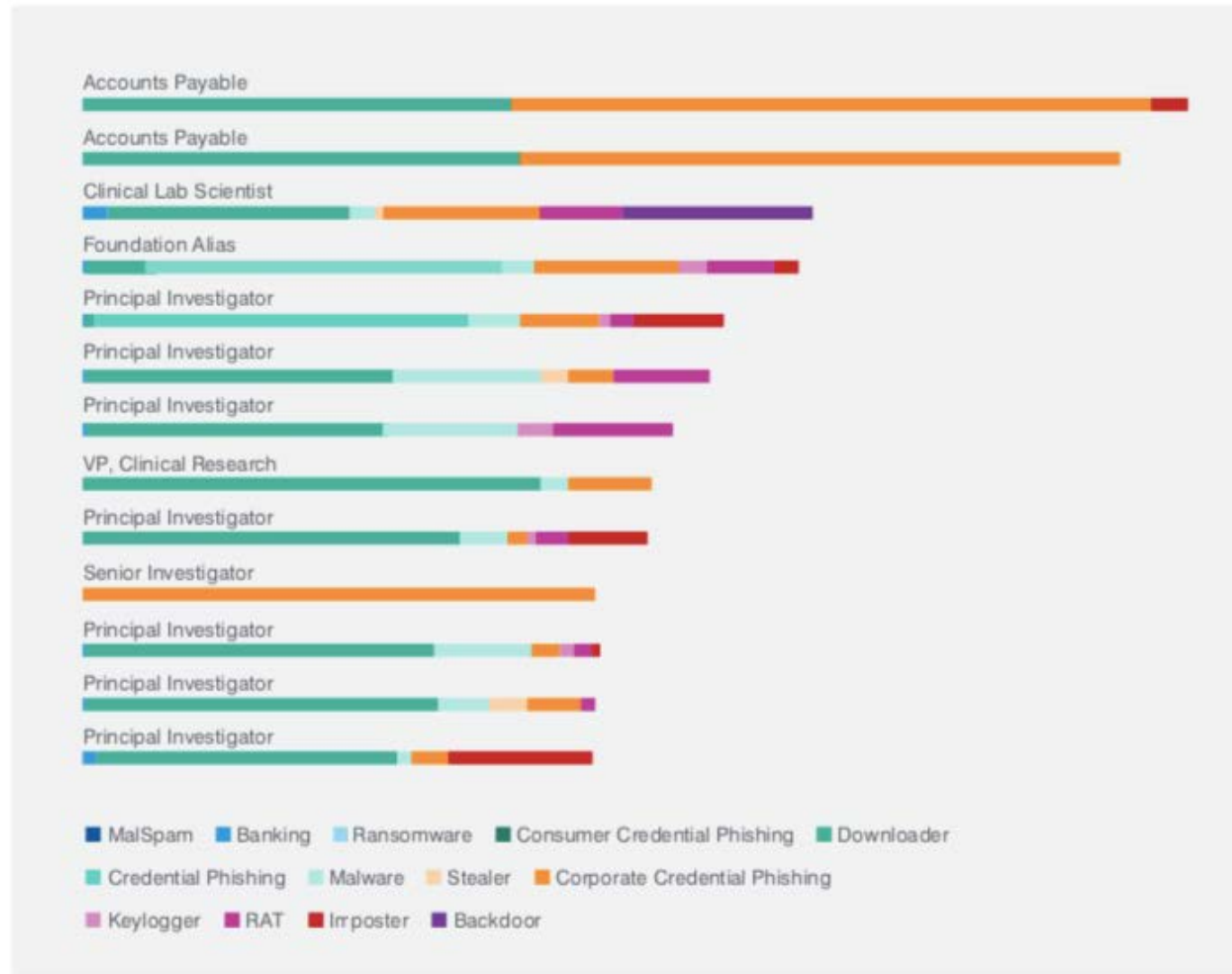


Who in Healthcare is Being Attacked

Getting to Know Healthcare's Very Attacked People

| | | | |
|----------------------|---|---|---|
| Pharmaceuticals |  Executives |  Public Affairs |  Email Alias |
| Large Health Systems |  Clinical Staff |  Rehab Therapy |  Executives |
| Insurers |  Patient Support |  Executives |  Finance |
| Children's Hospitals |  Research Teams |  Clinical Staff |  Accounts Payable |
| Teaching Hospitals |  Professors |  Alumni |  Grants / Finance |

VAP Case Study – Children’s Hospital



- Large children’s hospital
- 20K email accounts
- Heavy focus on job titles associated to clinical research department
- Goal – intellectual property theft presumably

Top 20 Very Attacked Persons – 20+ Hospital IDN





Recommendations

Recommendations

- Adopt a **people-centric** security posture
- Use data on **who's being attacked** to influence security strategy
- **Train users** to spot and report malicious emails
- Deploy **robust email security** and ability to prevent exfiltration (**DLP**)
- Build strong business **email compromise defense** system
- Adopt **Zero Trust** to enable remote working
- **Isolate** risky websites, URLs, and “happy clickers”
- **Secure O365** and other cloud apps



Questions & Answers

A man and a woman are in a meeting room. The woman is pointing at a whiteboard covered in sticky notes. The man is holding a tablet and looking at the whiteboard. The word "proofpoint" is overlaid in the center of the image.

proofpoint®