proofpoint®

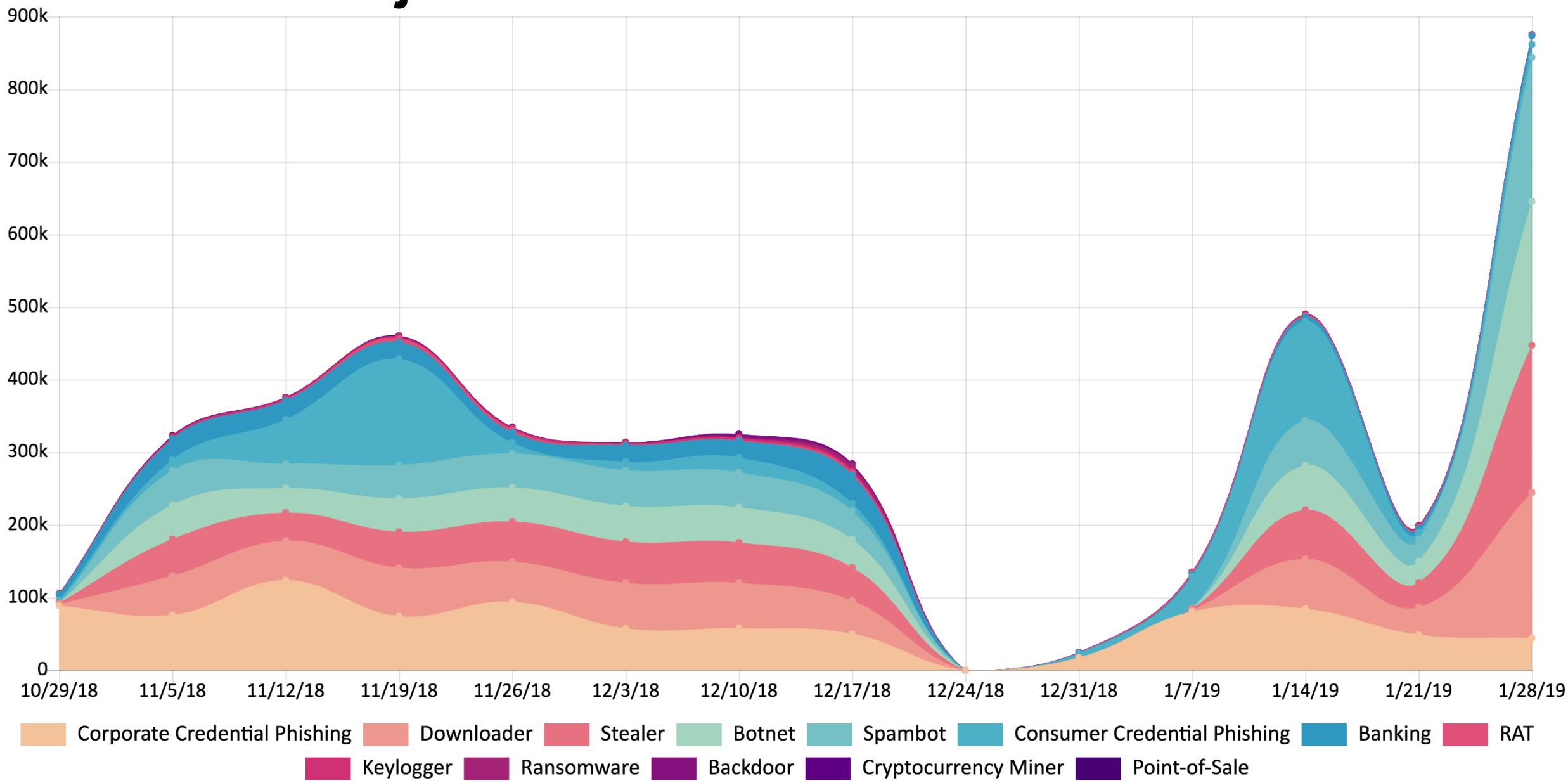
Building a People-Centric Security Strategy

Adenike Cosgrove

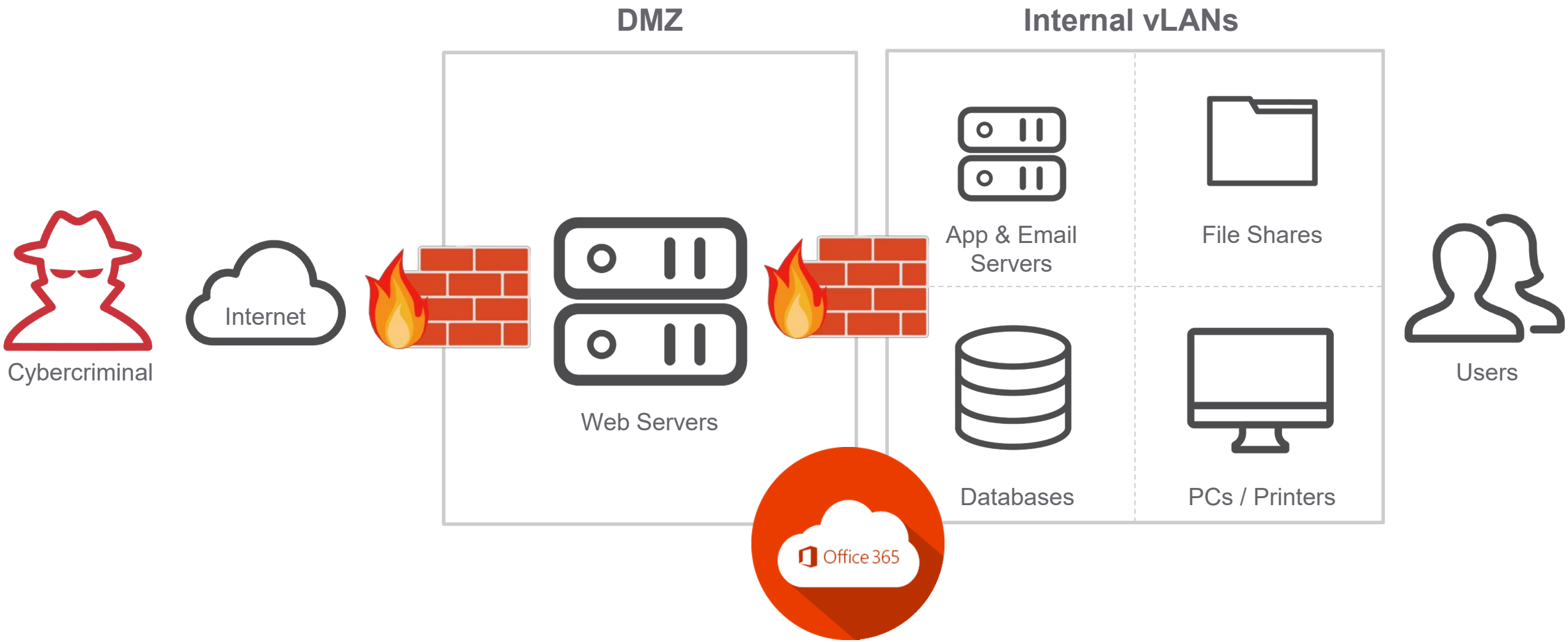
26 March 2019

bsi. International Cyber Resilience Exchange 2019

Attacker's Objectives: Global View



The Defender's View: Protect the Network



The Attacker's View: Target the Human Factor

Cybercriminal

High
Value Executive

James Diamante • Following
CEO at Bank Co
500+ connections
4000 followers

- VIP by role, access
- Thousands of connections
- Targeted by email fraud actors
- Impersonated to attack others

High
Access User

Joe Greene • 3rd
Loan Officer at Bank Co
500+ connections

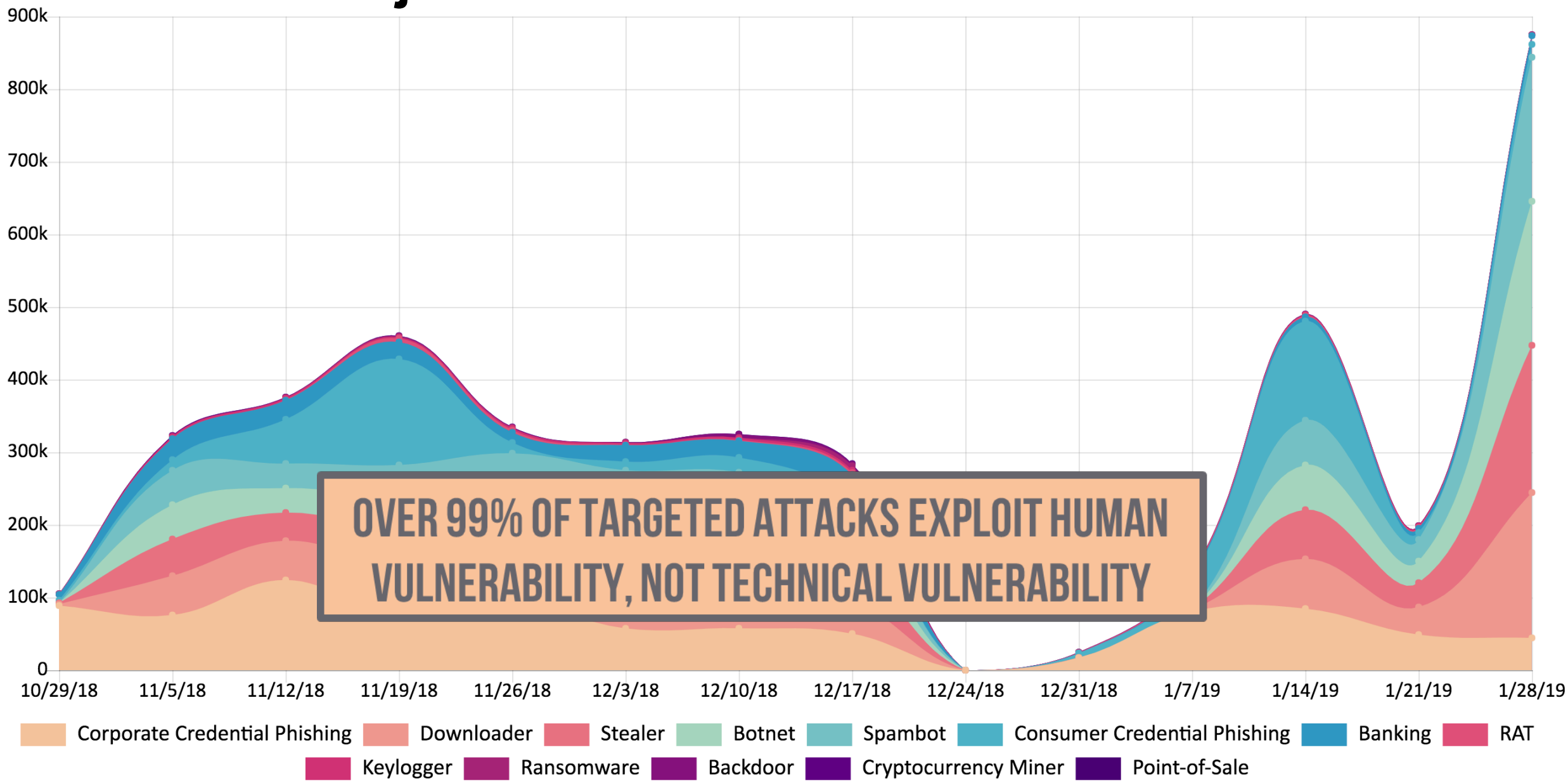
- VIP by access - Access to financial systems
- Targeted by financially motivated phishers

High
Access User

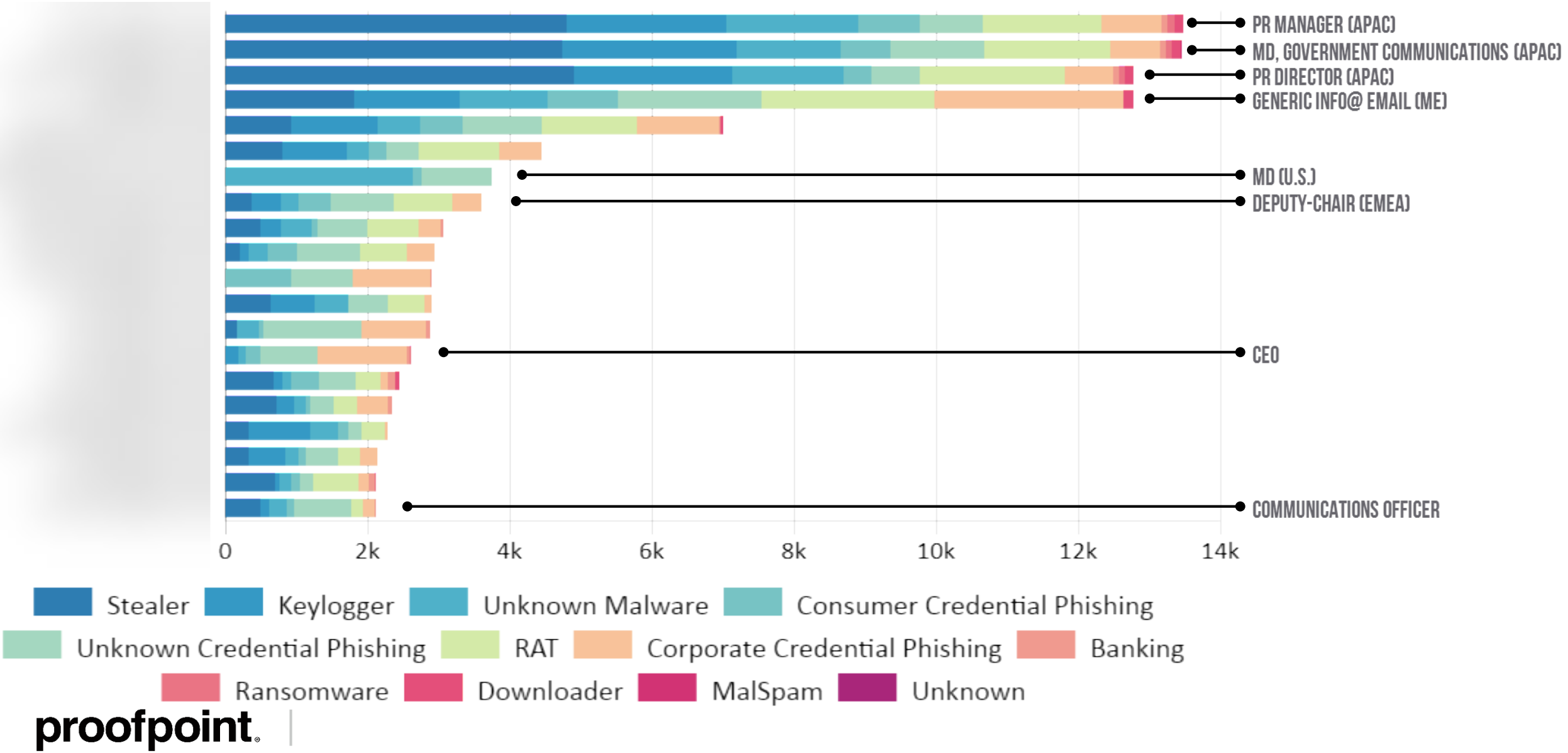
Jennifer Jones • 1st
Financial Filing Analyst at Bank Co
45 connections

- Creates and processes invoices for third party partners
- Impersonated to attack third party partners

Attacker's Objectives: Global View

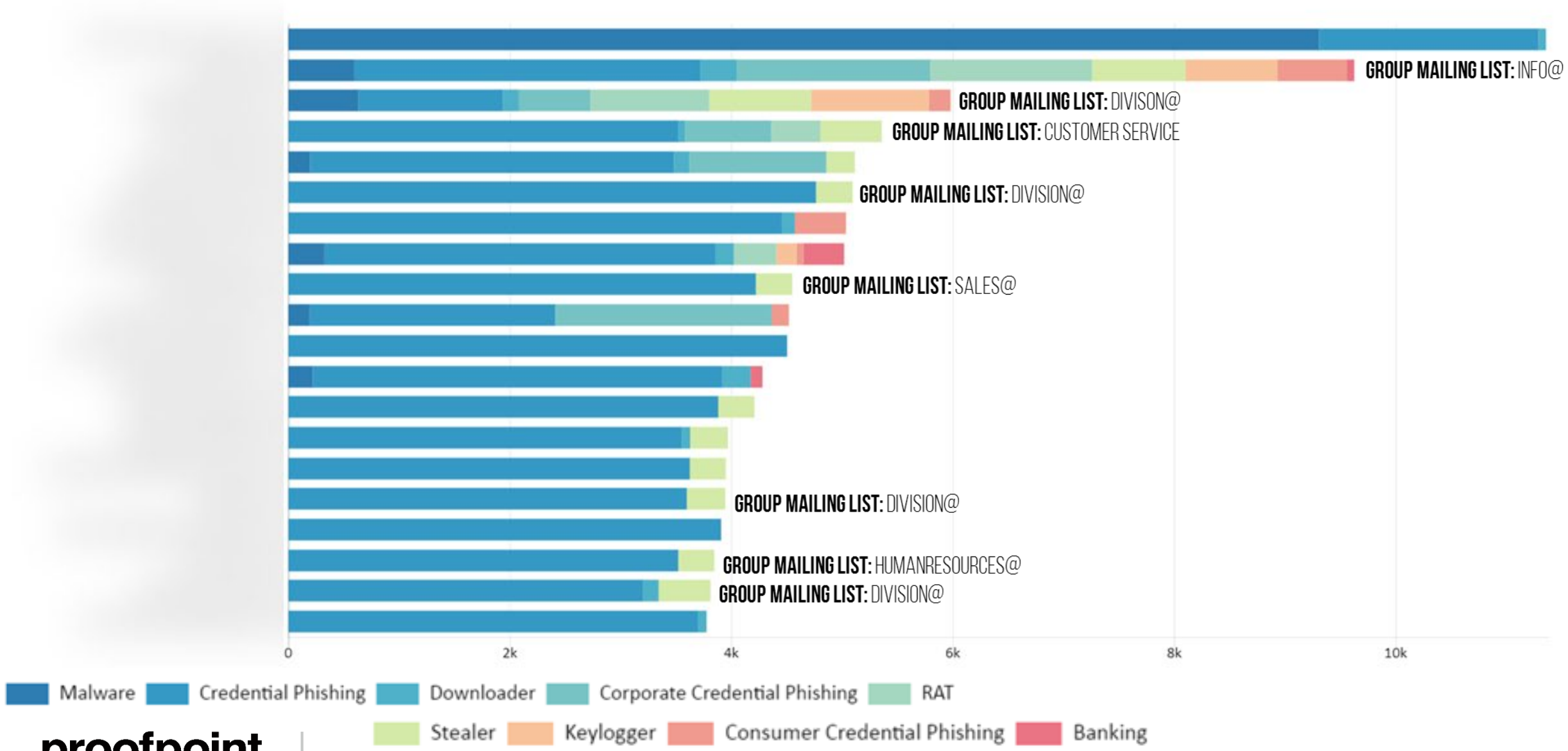


The Attacker's View: Global Advertising



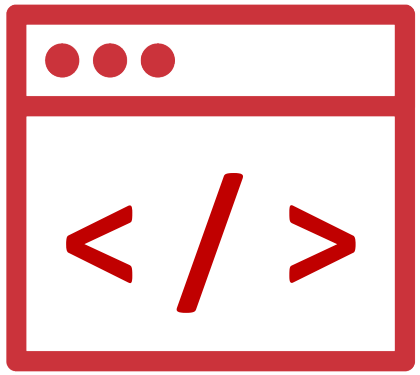
proofpoint.

The Attacker's View: European Retailer



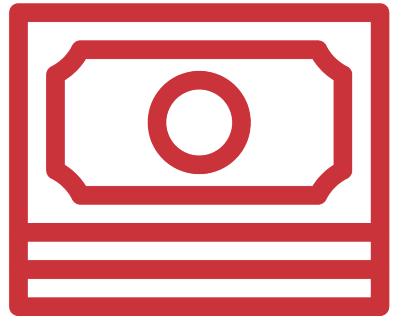
proofpoint.

How Attackers Use People



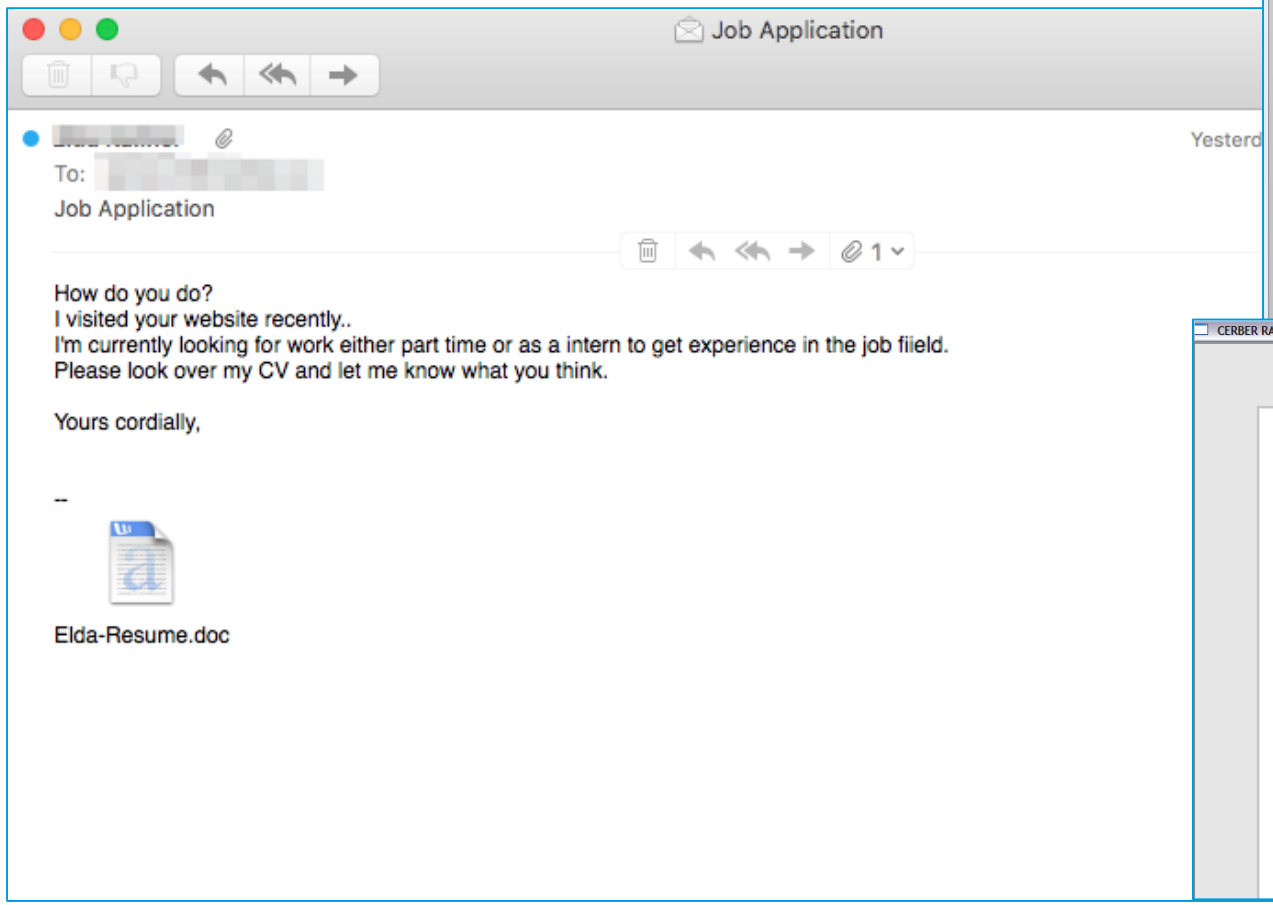
RUNNING ATTACKERS' CODE FOR THEM

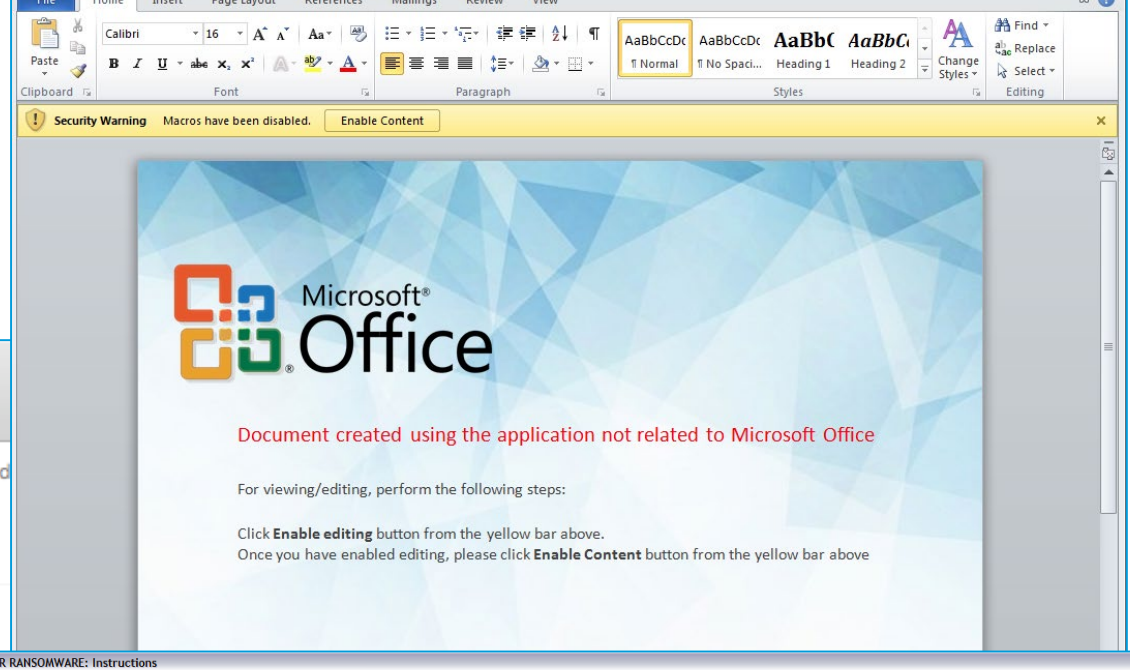
HANDING OVER CREDENTIALS TO THEM

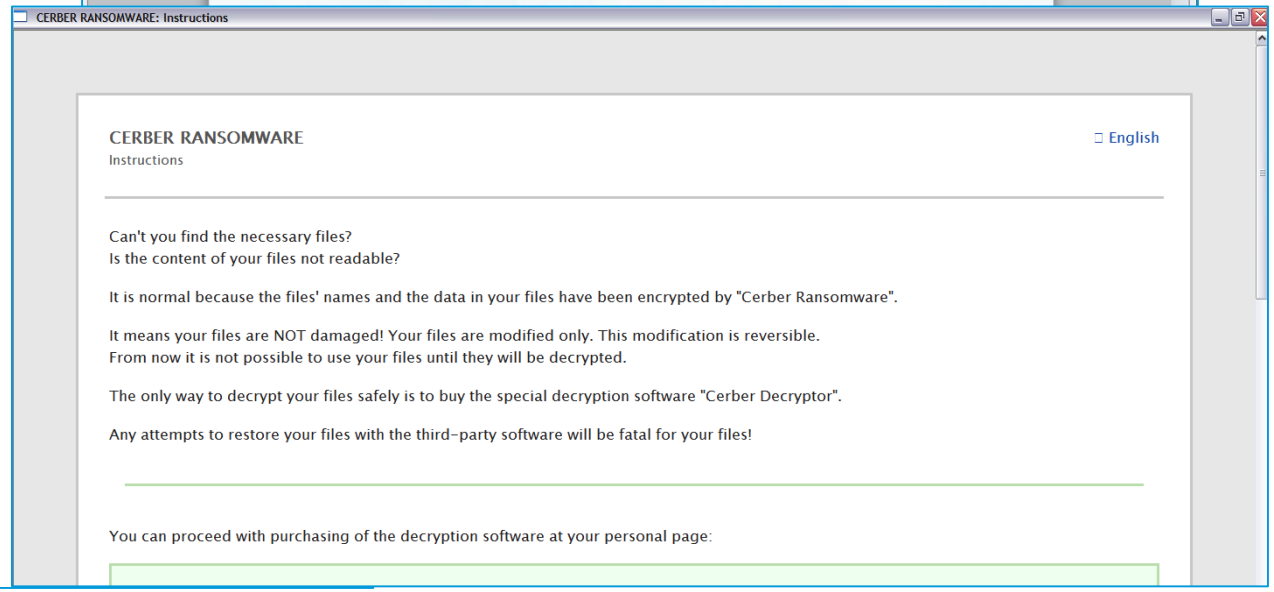


TRANSFER FUNDS OR DATA TO THEM

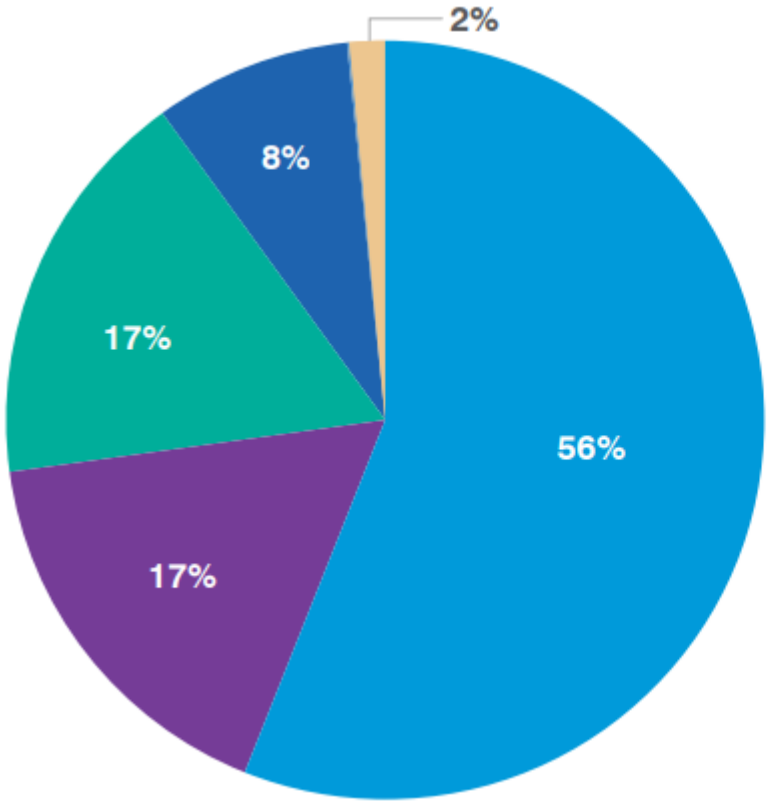
What is Ransomware?

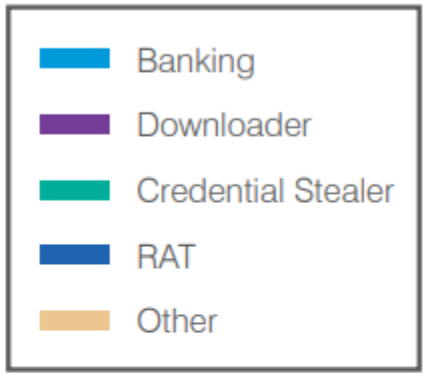






Criminals Pivot to Trojans – Ransomware Subsides





RANSOMWARE WAS VIRTUALLY ABSENT IN Q4 2018…

DRAMATIC Q4 INCREASES IN BANKING TROJANS & OTHER MALWARE.

What is Credential Phishing

Spoof trusted third parties, customers, or executives. Sent from lookalike domains

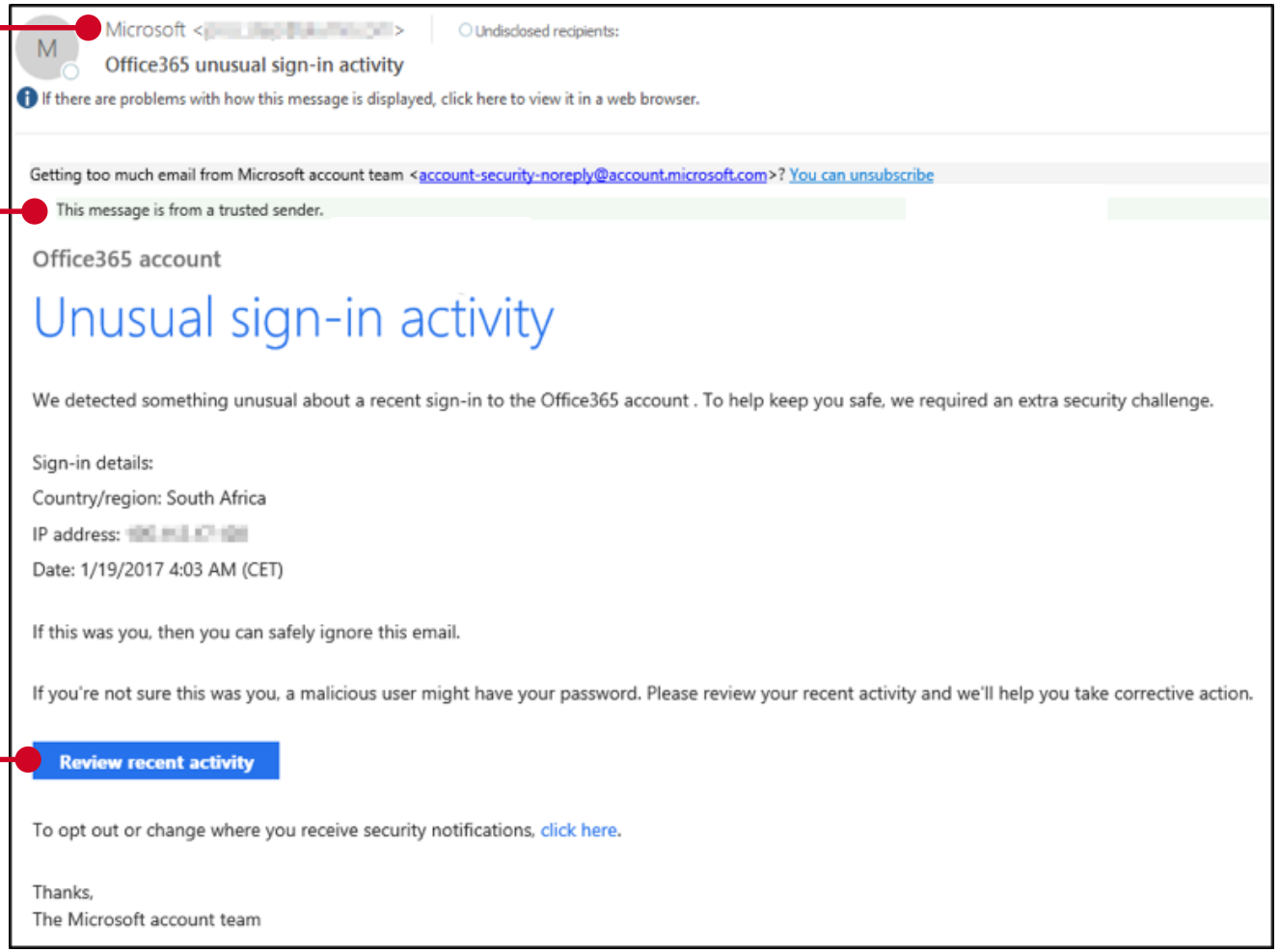
1

Claims to be secure

2

No malware to analyse

3

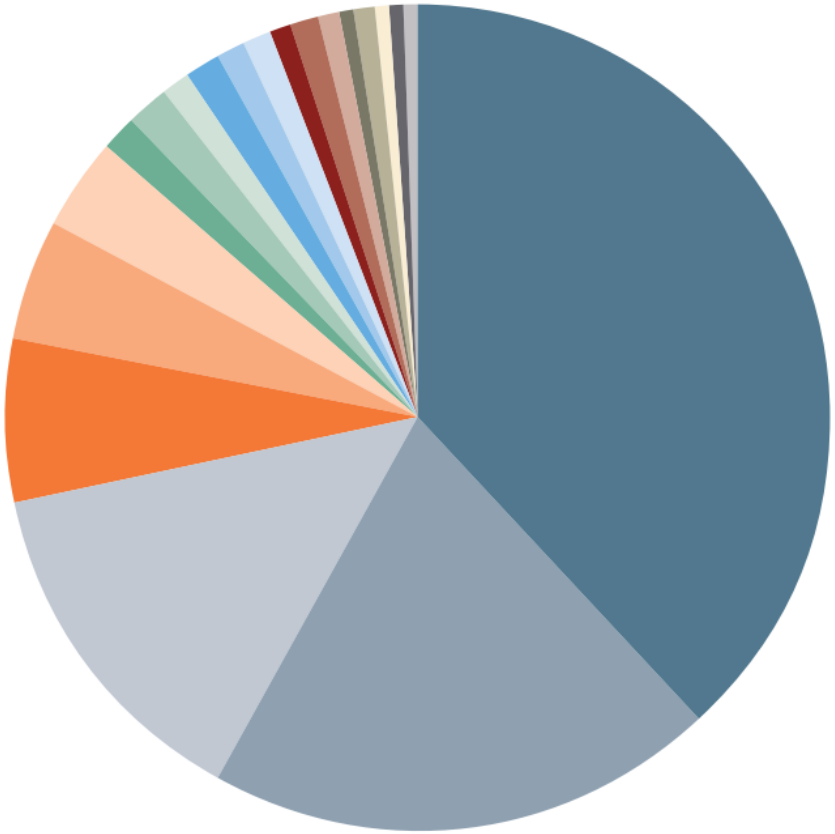


Hijacked site with good reputation

Visually convincing site

Trying to steal credentials

Criminals Target Users for Credentials



- Dropbox Account Phishing
- Financial Institution Phishing
- Generic Email Credential Harvesting
- Microsoft OWA Phishing
- Office 365 Account Phishing
- Adobe Account Phishing
- Google Drive Phishing
- Docusign Phishing
- Netflix Phishing
- PayPal Phishing
- Amazon Phishing
- Apple Account Phishing
- Microsoft Excel Online Phishing
- Linkedin Account Phishing
- Windows Settings Phishing
- Postal / Shipping Company Phishing
- MyEtherWallet Phishing
- Alibaba Phishing
- OneDrive Phishing
- Retail Phishing

WHILE NEW MALWARE OFTEN MAKES HEADLINES, CORPORATE CREDENTIAL **PHISHING VIA EMAIL INCREASED OVER 300%** BETWEEN Q2 AND Q3 2018

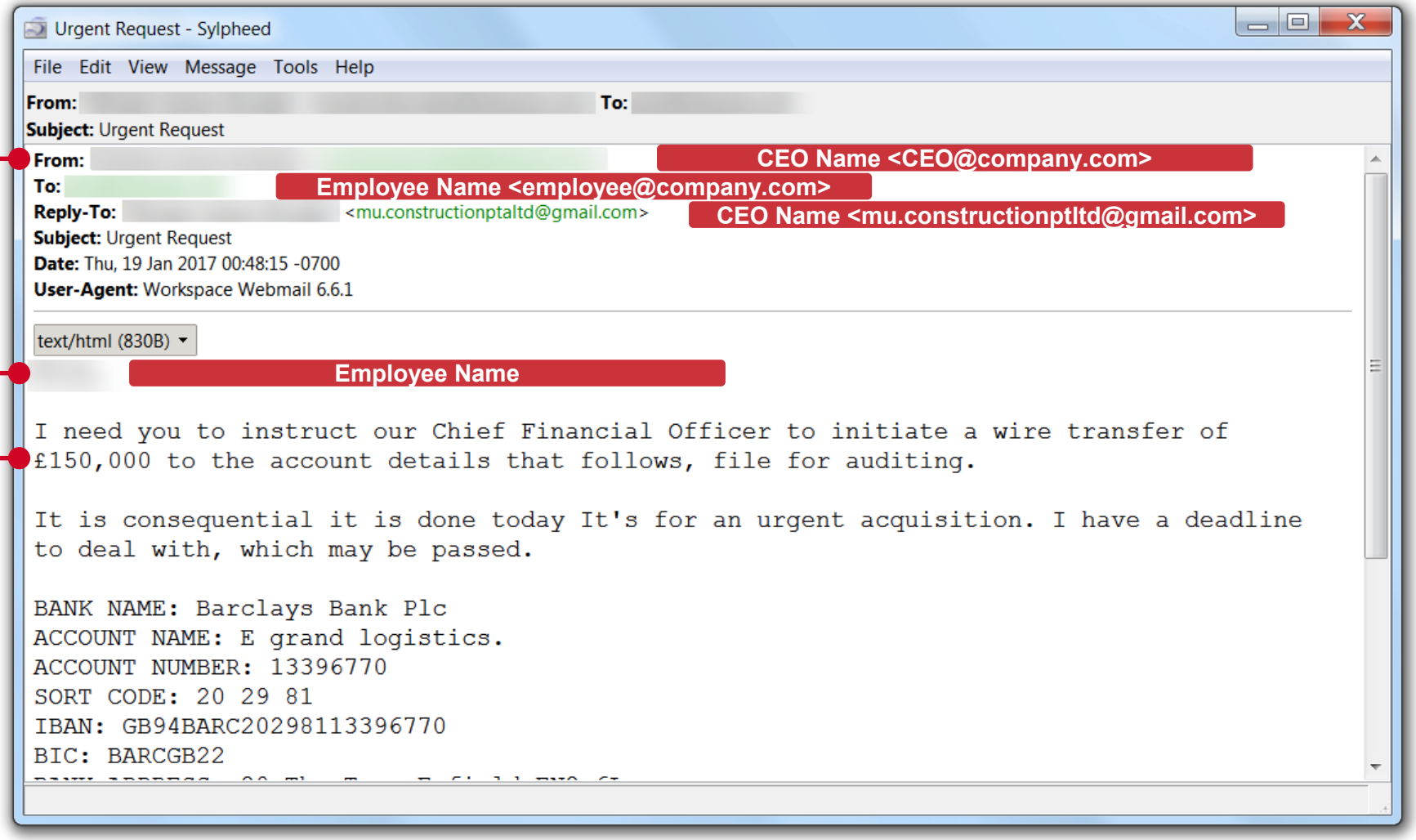
What is Business Email Compromise?

Impersonate corporate identities

Highly-targeted, low volume attacks

Aim to solicit:

- Fraudulent wire transfers
- Steal company data
- Steal credentials and other confidential information



Attacks Target Individuals, Not Infrastructure

90%

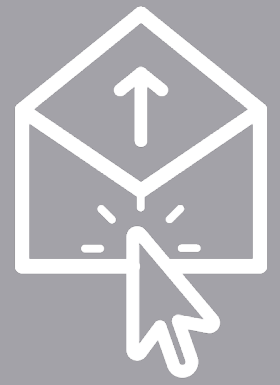
THREATS USE SOCIAL ENGINEERING, NOT VULNERABILITIES

90%+ rely on users to run malicious code.

37%

SHIFT TO CLOUD CREATES NEW THREAT VECTORS, DATA EXPOSURE

37% of companies breached via cloud apps.



$12.5B

BEC/EIP/IMPOSTOR EMAIL FRAUD BECOMES BOARD-LEVEL ISSUE

$12.5B losses from BEC/EAC since Oct 13.

Phishing Most Successful Infection Vector

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

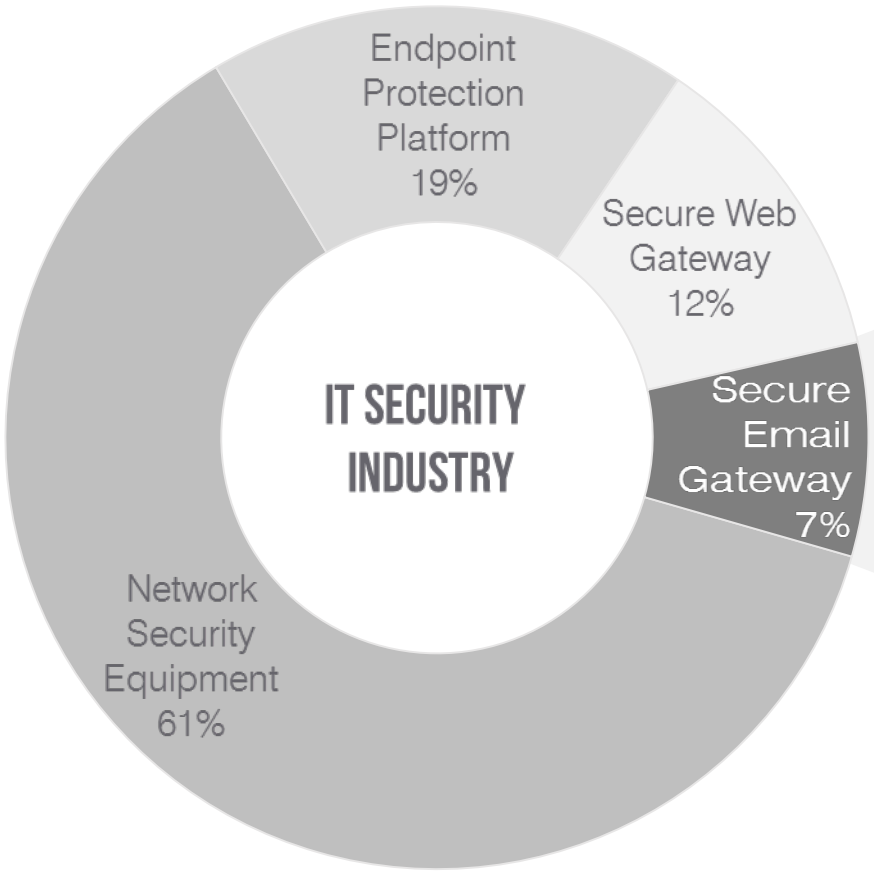
Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

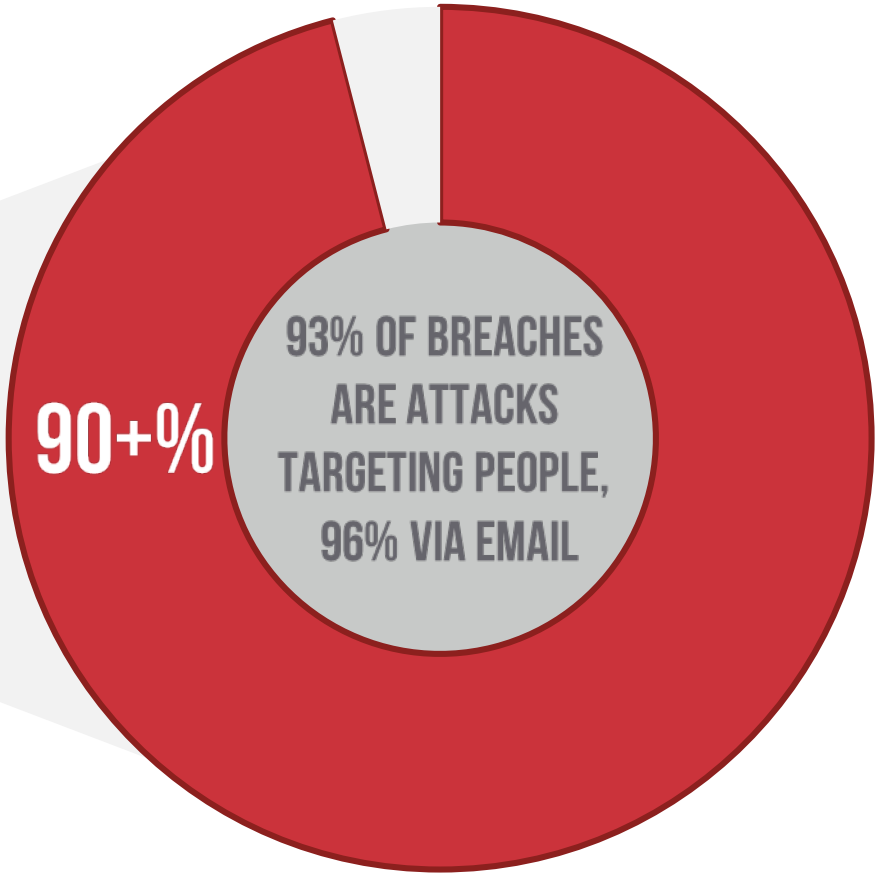
1. Malware
2. Web Based Attacks
4. Phishing
6. Spam

"THE SUCCESS OF [PHISHING] IS MANIFES
NEW RECORD IN DATA BREACHES REPOR

Source: ENISA 2018 Threat Report, 28 January 2019

Defenders Don’t Focus on People, Attackers Do





Source: Gartner Information Security Market* WW End-User spending 2018

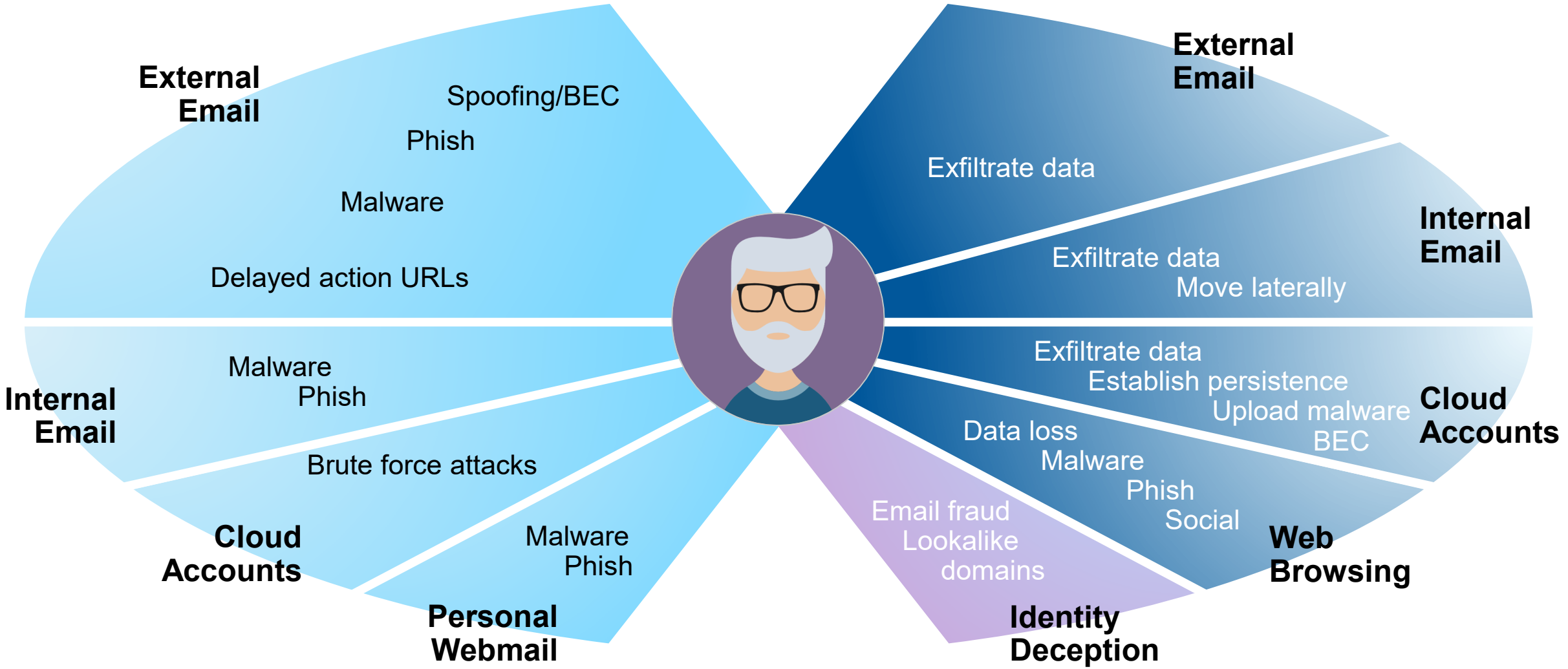
Source: Verizon DBIR

PEOPLE-CENTRIC
SECURITY

proofpoint®

PEOPLE-CENTRIC ATTACK VECTORS: INITIAL COMPROMISE

PEOPLE-CENTRIC ATTACK VECTORS: POST-COMPROMISE



PEOPLE-CENTRIC ATTACK VECTORS: BUSINESS ECOSYSTEM

Who Are Your VAPs?

Targeted by Threats

Receive highly targeted, very sophisticated, or high volumes of attacks

Work in High Risk Ways

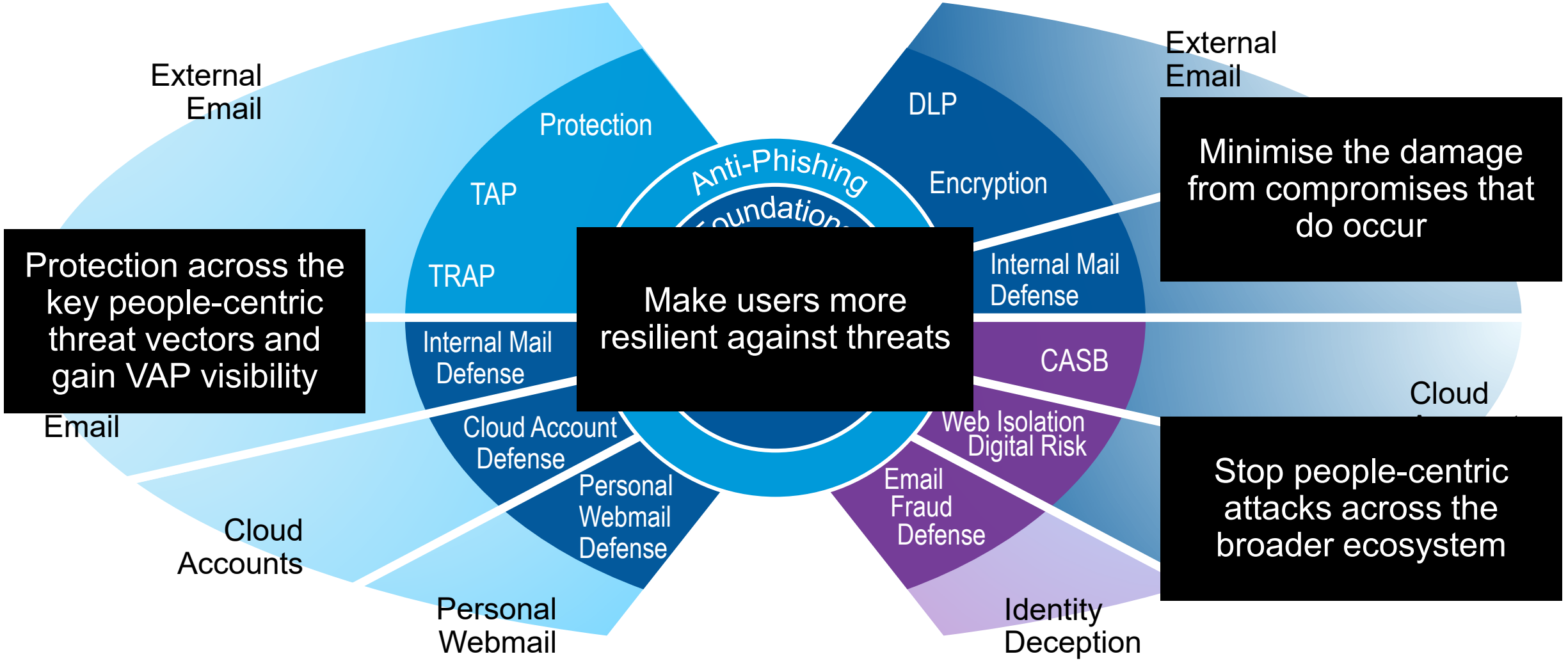
Clicks on malicious content, fails awareness training, or uses risky devices/cloud services

Access to Valuable Data

Can access or manage critical systems or sensitive data

PEOPLE-CENTRIC ATTACK VECTORS: INITIAL COMPROMISE

PEOPLE-CENTRIC ATTACK VECTORS: POST-COMPROMISE



PEOPLE-CENTRIC ATTACK VECTORS: BUSINESS ECOSYSTEM

proofpoint.

Learn More

@proofpoint

2018 Human Factor Report
https://www.proofpoint.com/it/human-factor-2018