SEEING THE ATTACKER’S VIEW: A PEOPLE-CENTRIC APPROACH TO THREAT PROTECTION

Gary Steele

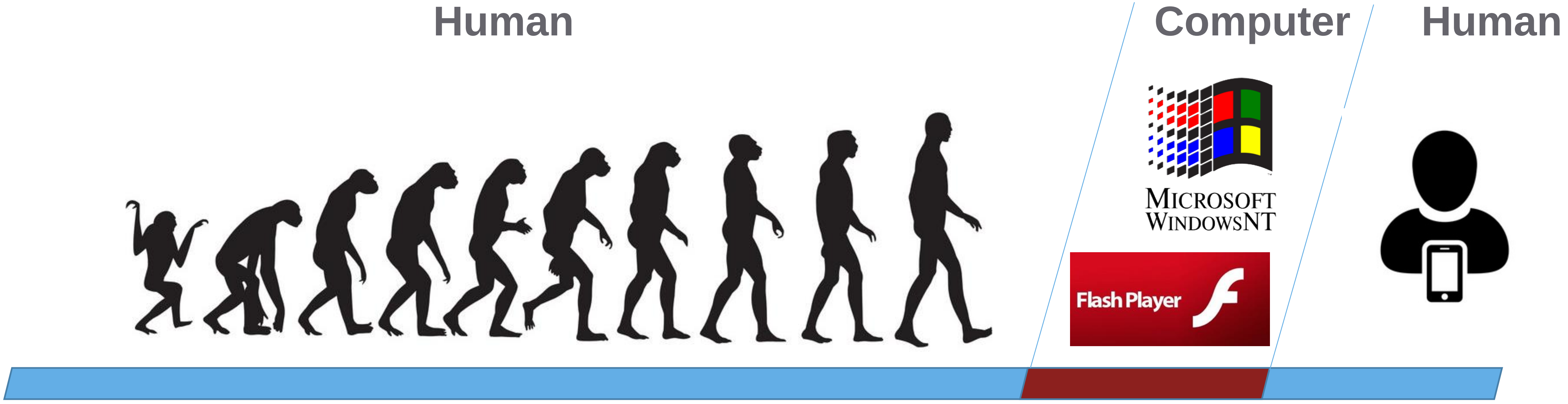
Chief Executive Officer, Proofpoint

October 11, 2019

People influence security more than technology or policy, and cybercriminals know how to exploit human behaviors.

**Gartner 2019 MQ for SACBT*

Which is Easier to Fool?



Human

Computer

Human

Dawn of time - 1995

1995 - 2015

2015 - present

Cloud Applications: It’s How People Work

Organizations use cloud apps across all functions

What CIOs estimate

30-40 apps

The reality

+1000

Source: CIO Magazine”

0365 is the #1 most-deployed cloud application

verizon

“Email is the most common attack vector (96%).”

Gartner

“40% of organizations will secure 0365 with a 3rd party solution.”

Source: Gartner Survey, ”Implementing Office 365”

User Trends

Internal users will consume more **apps delivered from outside** the enterprise network than from the inside.*

The future of work requires employees to be able to access the systems and data they need – from **wherever, whenever**.

Source: **Gartner,CARTA*

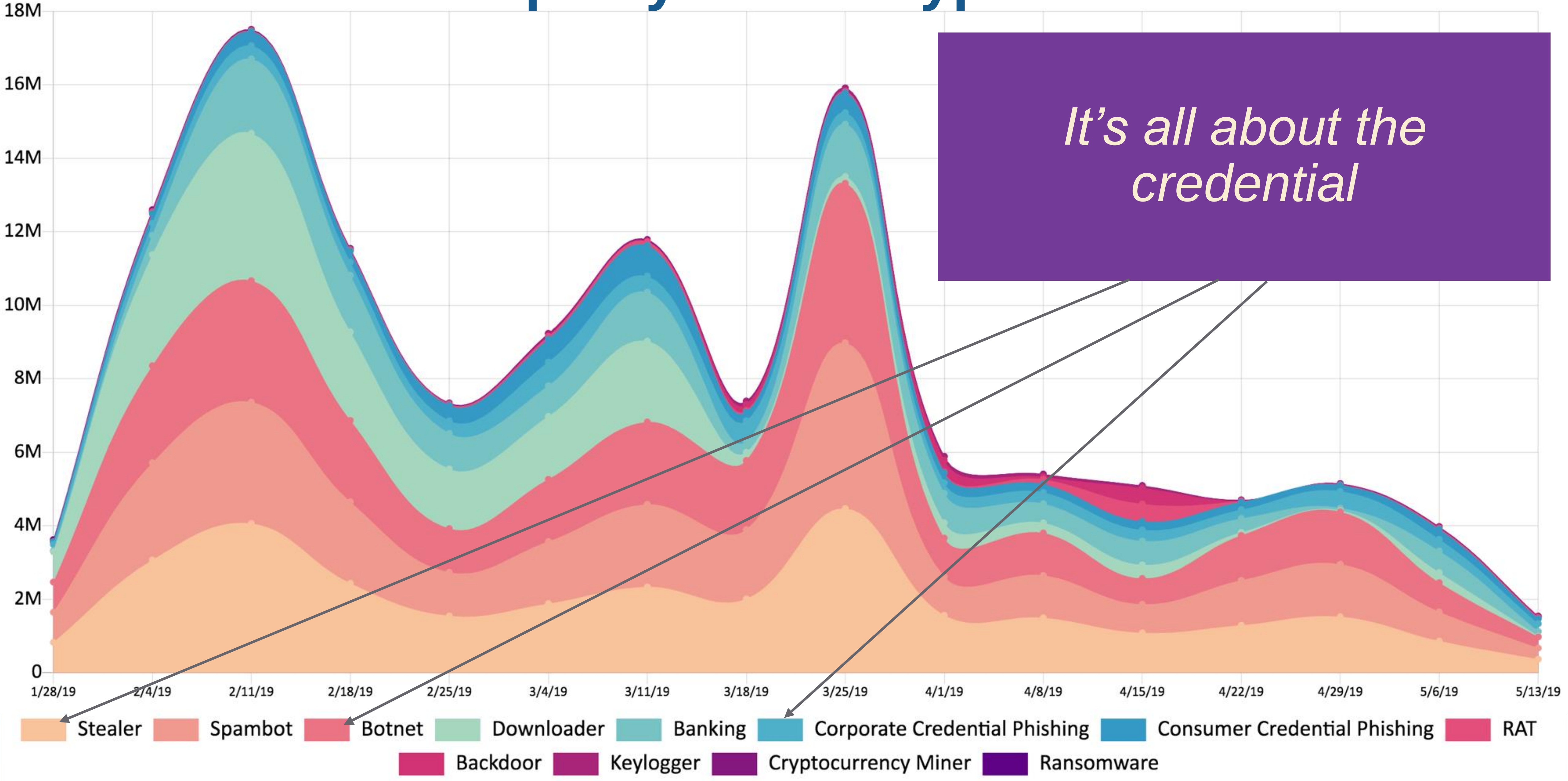
What Attackers Get People to Do

RUNNING ATTACKERS' CODE FOR THEM

HANDING OVER CREDENTIALS TO THEM

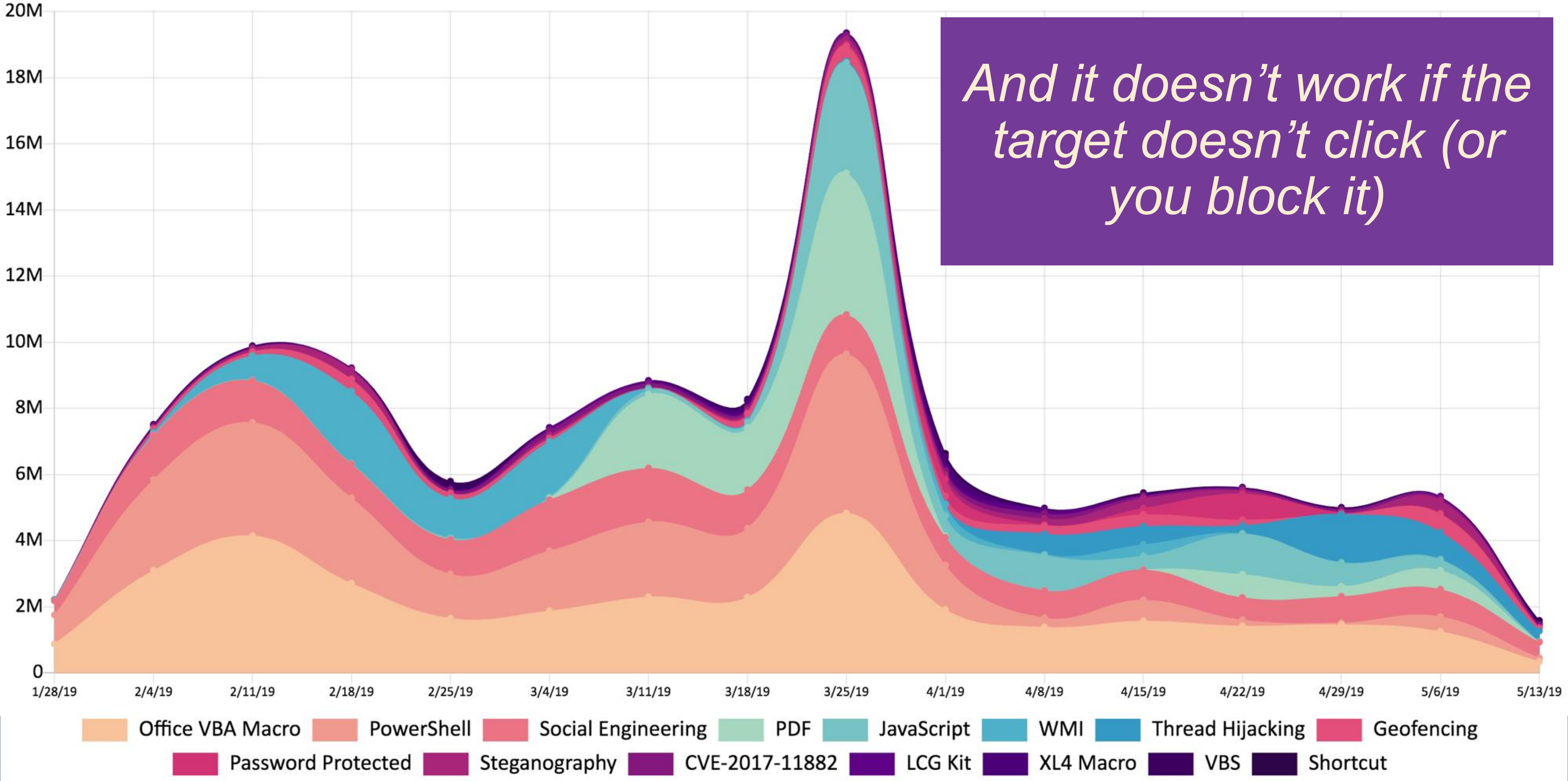
TRANSFER FUNDS OR DATA TO THEM

Threat Landscape by Attack Type



It’s all about the credential

Threat Landscape by Exploit Type



And it doesn’t work if the target doesn’t click (or you block it)

Attacks increasingly target people, not infrastructure

THREATS USE SOCIAL ENGINEERING, NOT VULNERABILITIES

99%+

Malware attacks rely on user to run malicious code

300%+

Increase in corporate credential phishing

Source: Proofpoint Threat Data.

SHIFT TO CLOUD CREATES NEW THREAT VECTORS, DATA EXPOSURE

Account takeover of cloud apps is a growing problem

63% Orgs exposed to targeted attacks

37% Orgs detected successful breach

Source: Proofpoint Threat Data.

EMAIL FRAUD IS A BOARD-LEVEL ISSUE

$12.5B+

Direct losses worldwide (Oct 2013–May 2018)

78,617

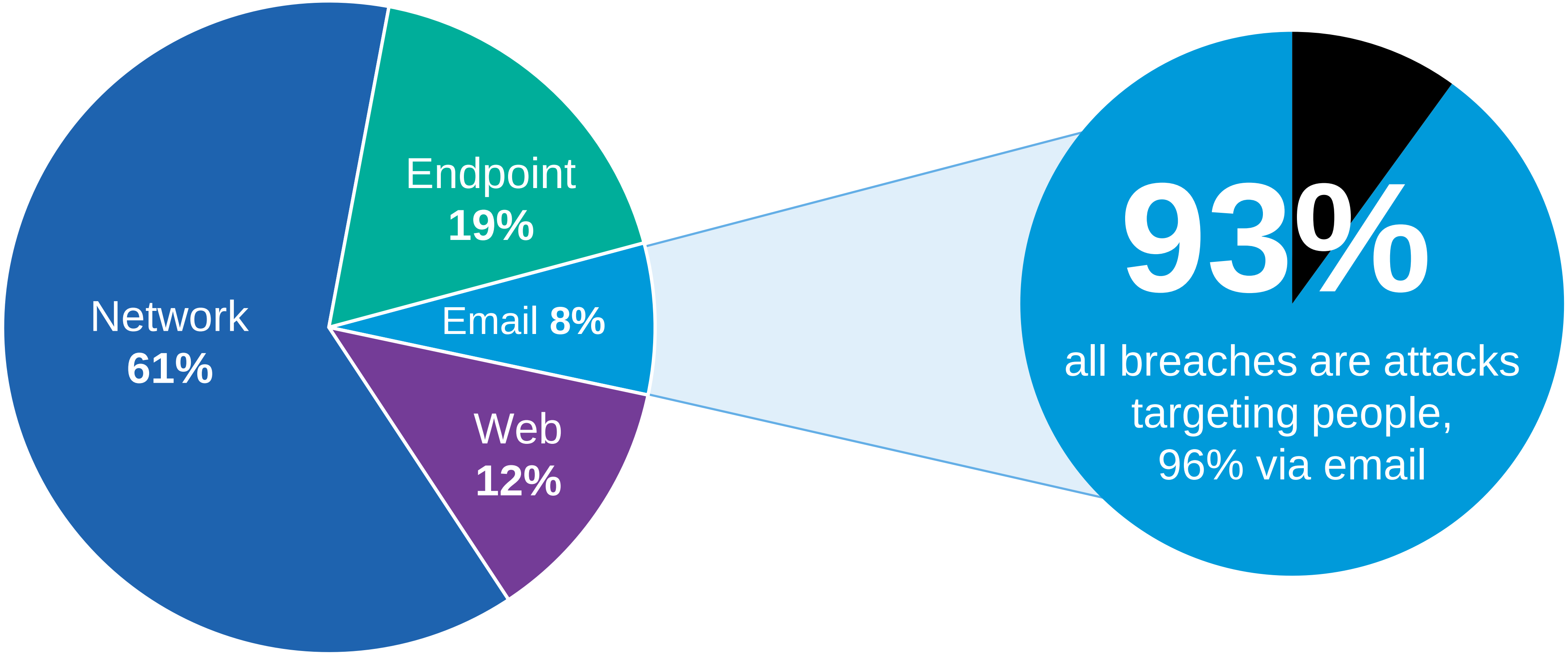
Incidents worldwide

Source: FBI.

Defenders don’t focus on people, attackers do

SECURITY SPENDING

ATTACK VECTORS

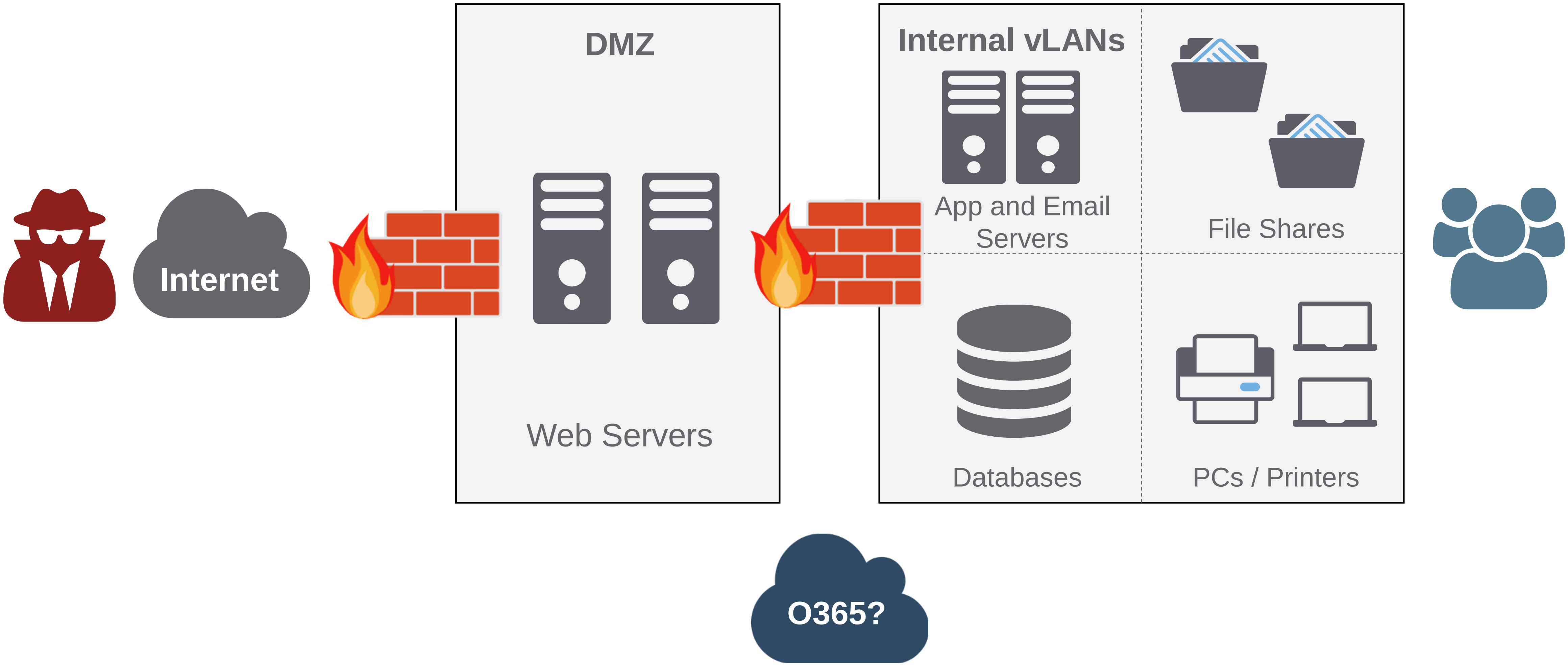


all breaches are attacks targeting people, 96% via email

Source: Gartner Information Security, Worldwide 2016 – 2022, 1Q 2018 update (2018 forecast)

Source: 2018 Verizon DBIR

Traditional Info Sec Point of View: Infrastructure



The Cybercriminal’s Point of View: People

jbarker@bank.com

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

lbream@bank.com

- Interacts and processes payments from clients
- Impersonated to attack third-party partners

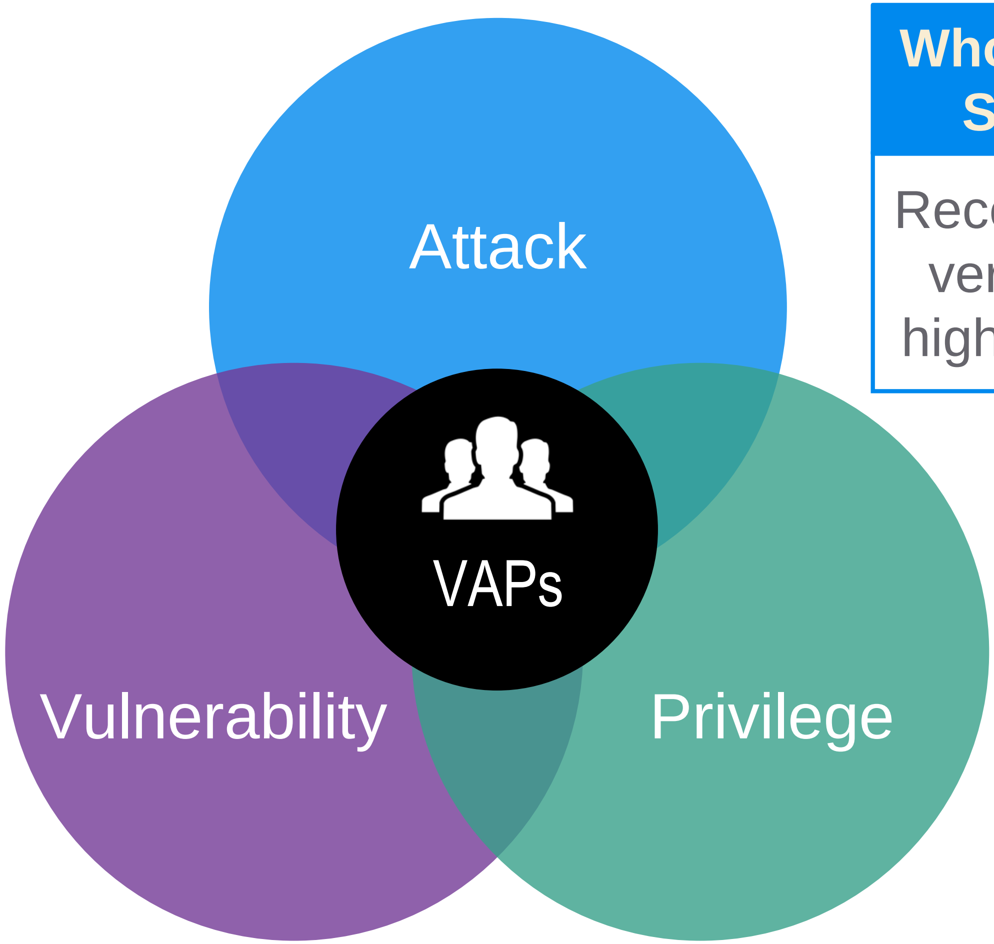
rhendricks@bank.com

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

Who are your Very Attacked People (VAPs)?

Who is Likely to Fall for those Threats?

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



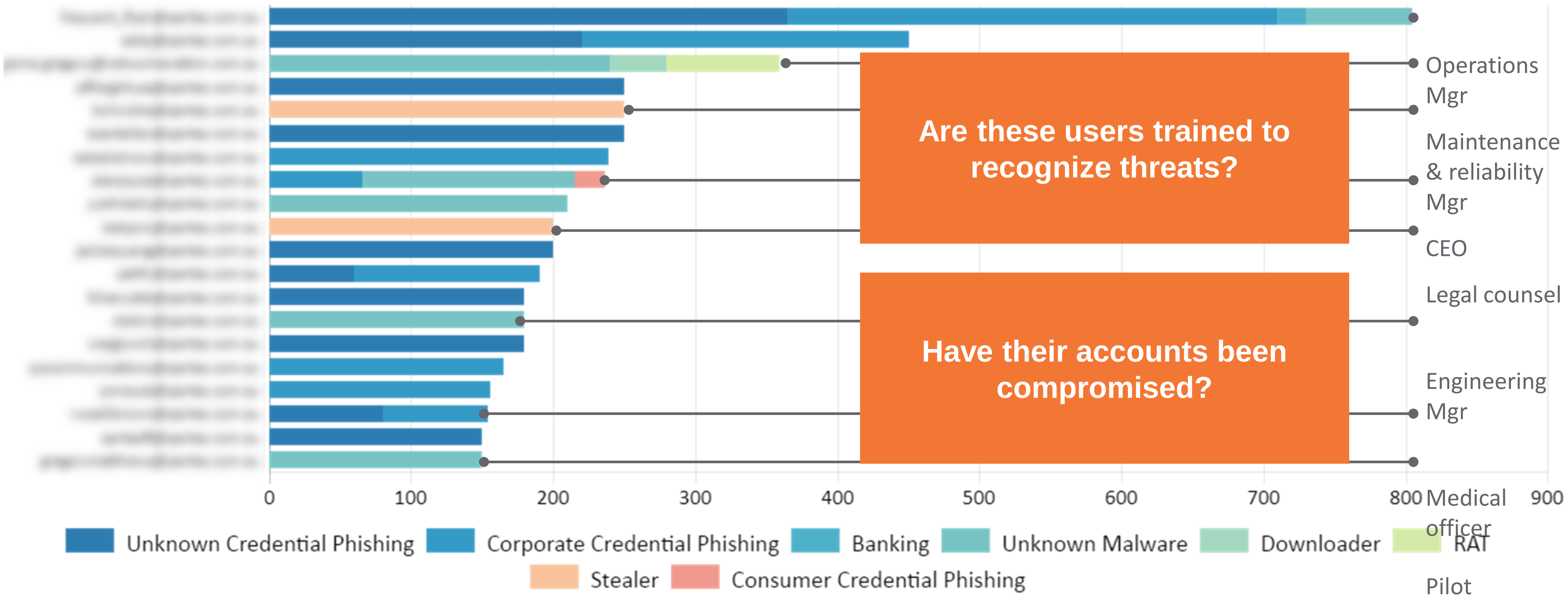
Who Gets Targeted by Serious Threats?

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

Who Represents Risk to the Organization?

Can access critical systems or sensitive data, or can be a vector for lateral movement

VAP View: Global Manufacturing Company



Are these users trained to recognize threats?

Have their accounts been compromised?

Operations Mgr

Maintenance & reliability Mgr

CEO

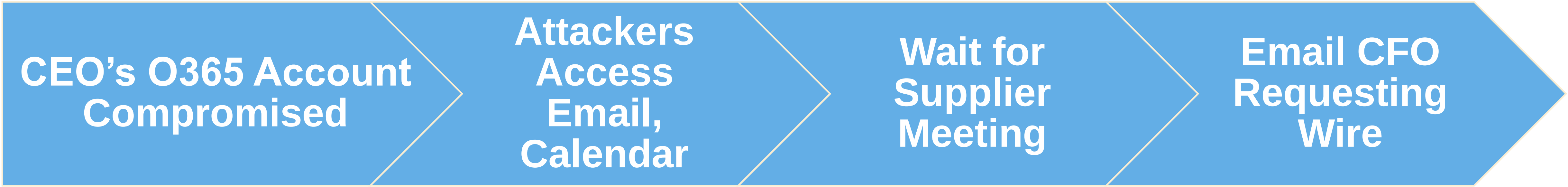
Legal counsel

Engineering Mgr

Medical officer

Pilot

Compromised Account Risk: How It Works



CEO’s O365 Account Compromised

Attackers Access Email, Calendar

Wait for Supplier Meeting

Email CFO Requesting Wire

From: Real CEO
To: Real CFO
Stuck in this meeting. Can you send a wire to acct 5551212? It’s the last thing we need to close the deal.

People-Centric Visibility Drives Better Protection

lbream@bank.com

Laurie Bream

Financial Advisor at Bank Co
500+ connections

Very Attacked People (VAP) Scores

VULNERABILITY

MEDIUM

Phish Simulation test: no action
Risky device / network use: yes
MFA: inconsistent

ATTACK

HIGH

Max threat: 850 (top 10%)
30 day total: 9,143 (top 5%)

PRIVILEGE

HIGH

VIP: yes
Sensitive data: yes, CASB DLP
AD Score: High

Adaptive Controls

+ Access Control

CASB: steps up authentication

+ Threat Control

Email Protection: turn on classifiers

+ Training Control

Training: data protection

proofpoint®