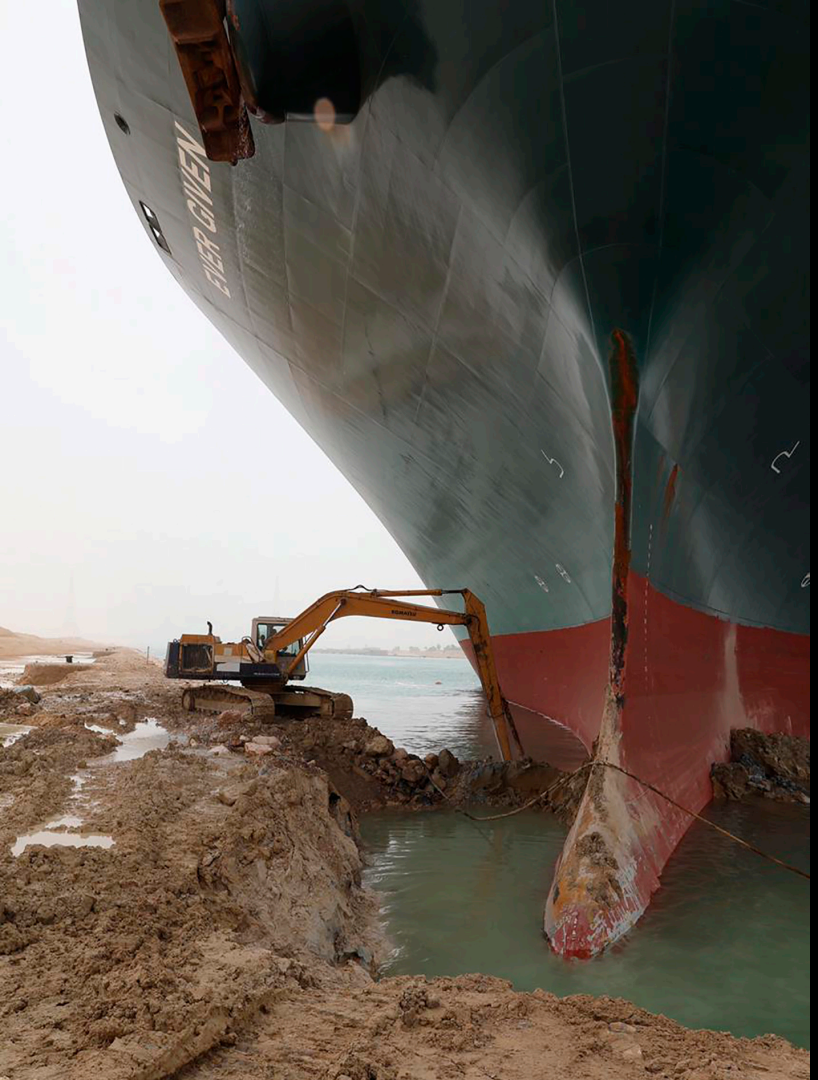
A people-centric approach to security.

proofpoint.

Adenike Cosgrove

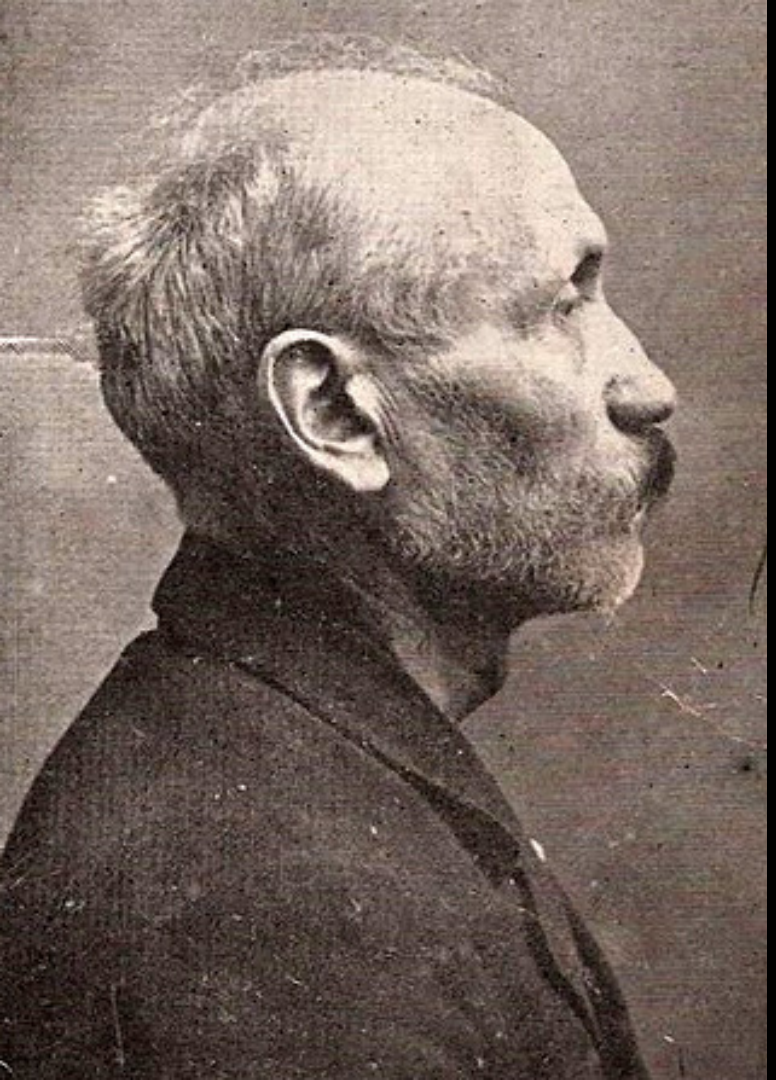
VP, Cybersecurity Strategy



“Egypt’s canal chief says human error could be behind ship’s grounding.”

proofpoint.


STADT-KAFFEE
STADT-KAFFEE
STADT-KAFFEE
EMIL RÖGENER
Waldorf-Astoria Cigarettes
Café Kropcke



"Friedrich Wilhelm Voigt masqueraded as a military officer, rounded up soldiers, and 'confiscated' 4,000 marks from a municipal treasury."

Donna-Marie Cullen 🎗️🌻 @DonnaCullen85 · May 17, 2021

HSE cyberattack ‘stole my end goal’, says cancer patient.

I’m just one of thousands of patients effected by this horrible cyberattack on the HSE.

@IrishTimes

irishtimes.com

HSE cyberattack ‘stole my end goal’, says cancer patient

Woman (36) due to finish treatment on May 31st but now has ‘no idea’ when she’ll be seen

“I got a call at lunchtime and was told that my radiation wouldn't be going ahead because of the cyber-attack.”

proofpoint.

It started with a phish

Anatomy of the ransomware (or BEC, or data theft) attack

Initial access

Attacker looks for a way into the organisation

18 March 2021
User opened malicious Microsoft Excel file attached to a phishing email sent on 16 March 2021.

Consolidation & preparation

Attacker attempts to gain access to critical devices and server admin

18 March 2021 – 14 May 2021
Attacker operated in network over eight-week period.

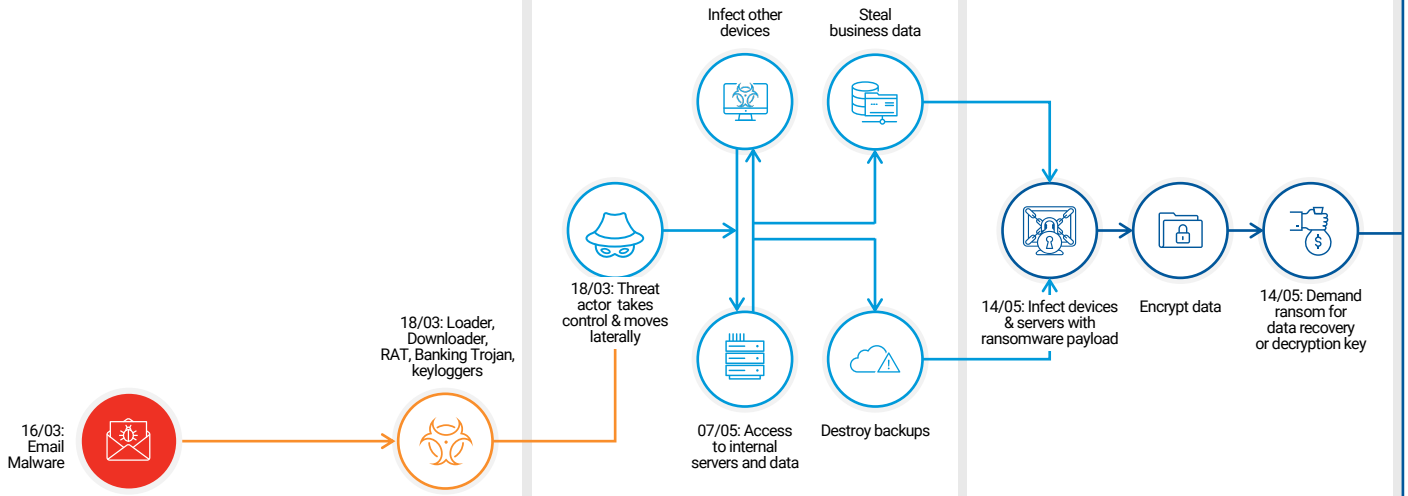
Ransomware launch

Once all systems identified, infected, and information collected, criminal then sends ransomware payload

14 May 2021
Detonation of Conti ransomware which caused widespread IT disruption.

Impact on target

Attacker steals and encrypts data, then demands ransom



“They don't do stages of sarcoma. You either have sarcoma, or it has spread, and if it has spread, it is terminal.

“For me it was the worry. If there was even a minute chance of a crumb of this cancer left in my head, that it would just start to multiply and my radiation plan would need to be completely revised.”

proofpoint.

“We got into your network through phishing. The email with the malicious attachment was opened by an employee... the user is asked to include the document's macro to display the content.

#Solution: Make it impossible to perform such an attack!
#How? You should figure it out for yourself…”

Systemic risk is people-centric risk.

85% of data breaches involved a human element, just 3% involved a technical vulnerability.

verizon

75% of ransomware attacks start with email.

paloalto NETWORKS

95% of security breaches are human related.

WORLD ECONOMIC FORUM

“Had we known that what was true nine years ago would still be true today, we could have saved some time by just copying and pasting some text.

Oh well, maybe in another nine years things will change for the better.”

verizon DBIR

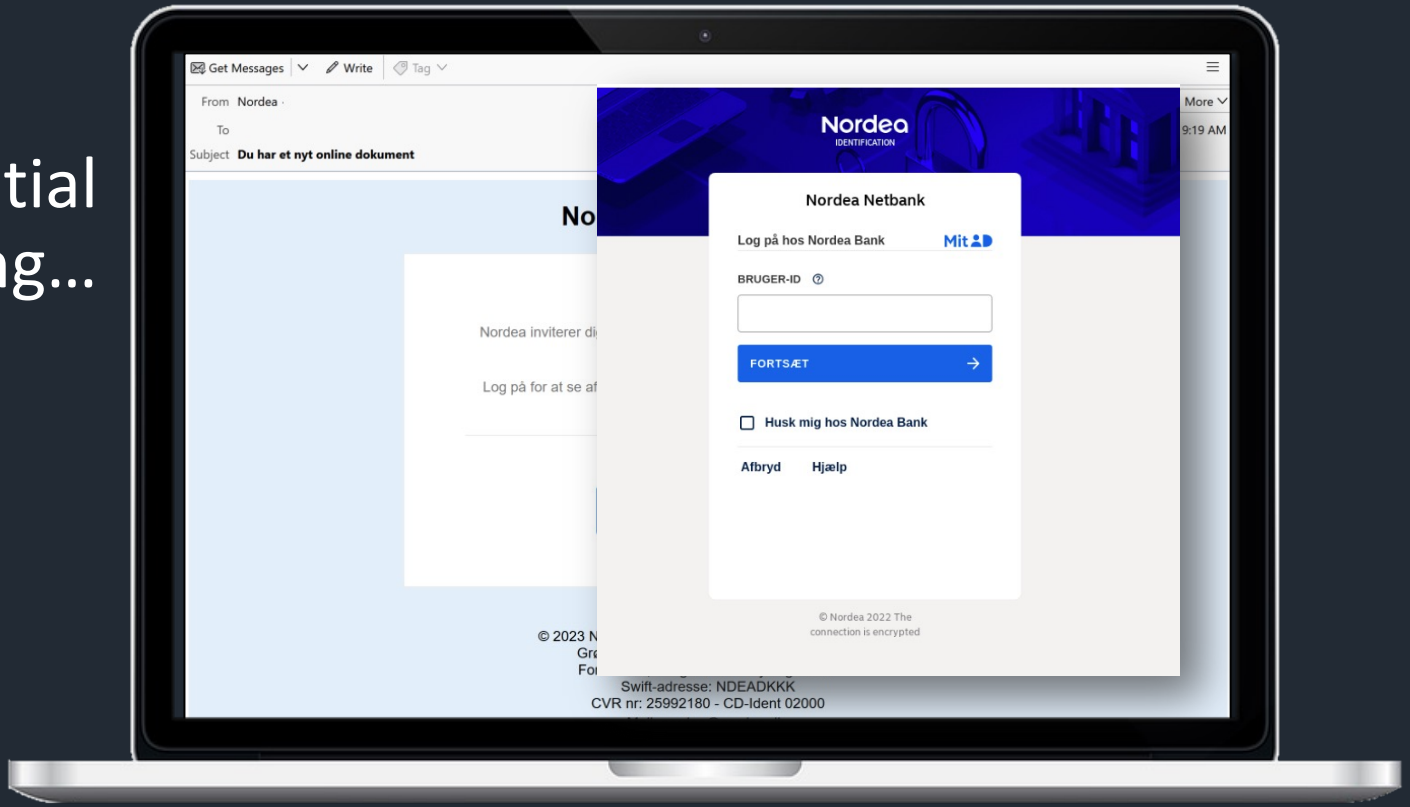
Attackers don’t hack in… they log in

RUNNING ATTACKER’S CODE FOR THEM

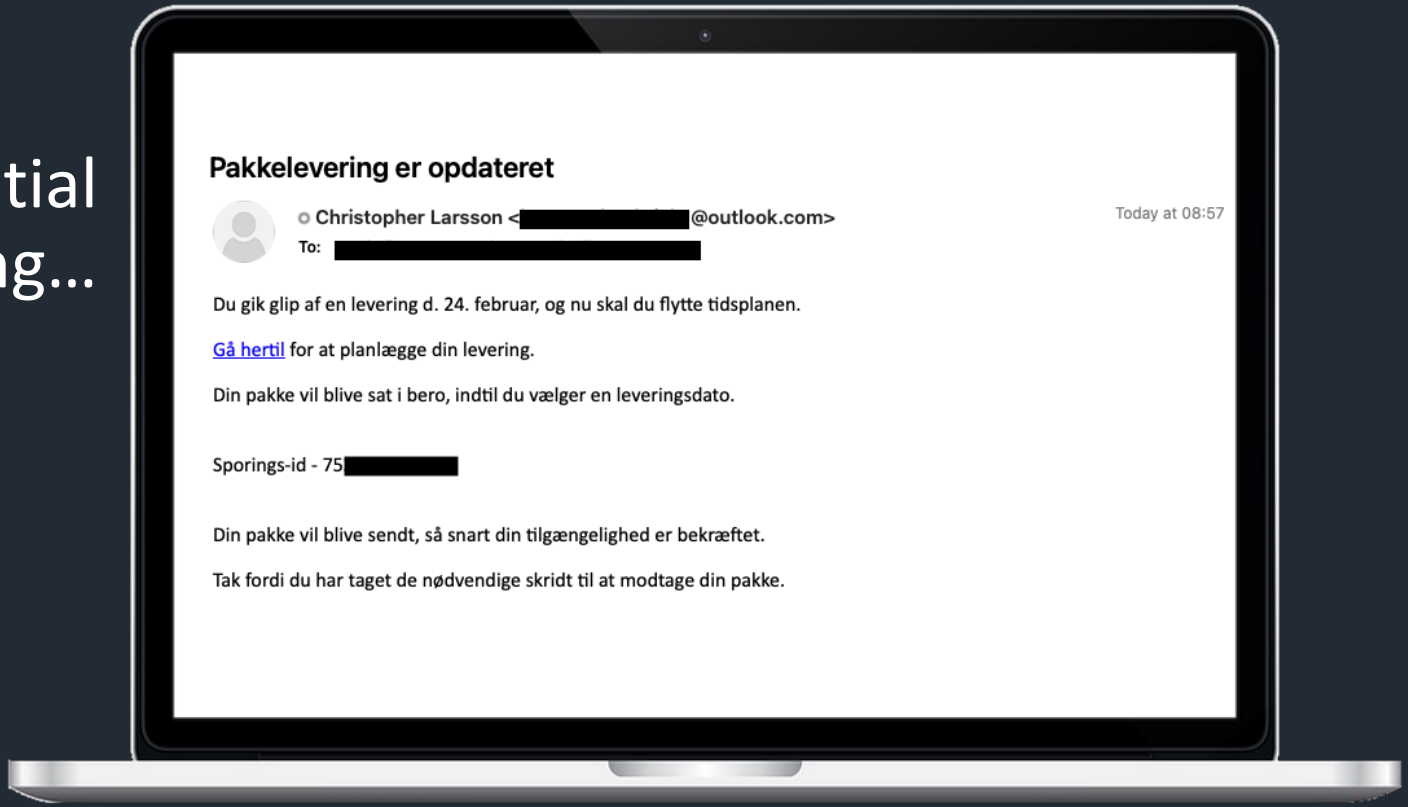
HANDING OVER CREDENTIALS TO THEM

TRANSFER FUNDS OR DATA TO THEM

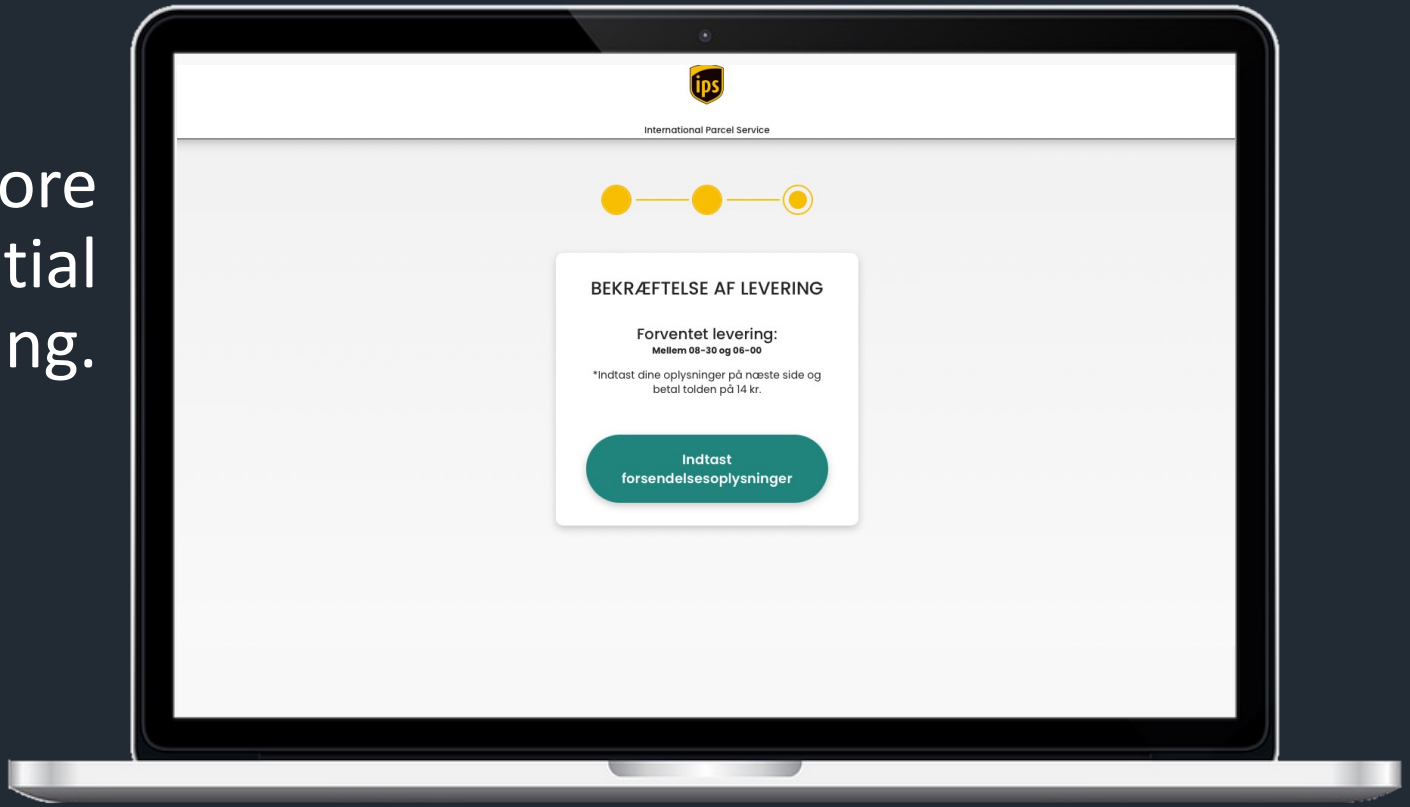
Credential phishing…



…credential phishing…

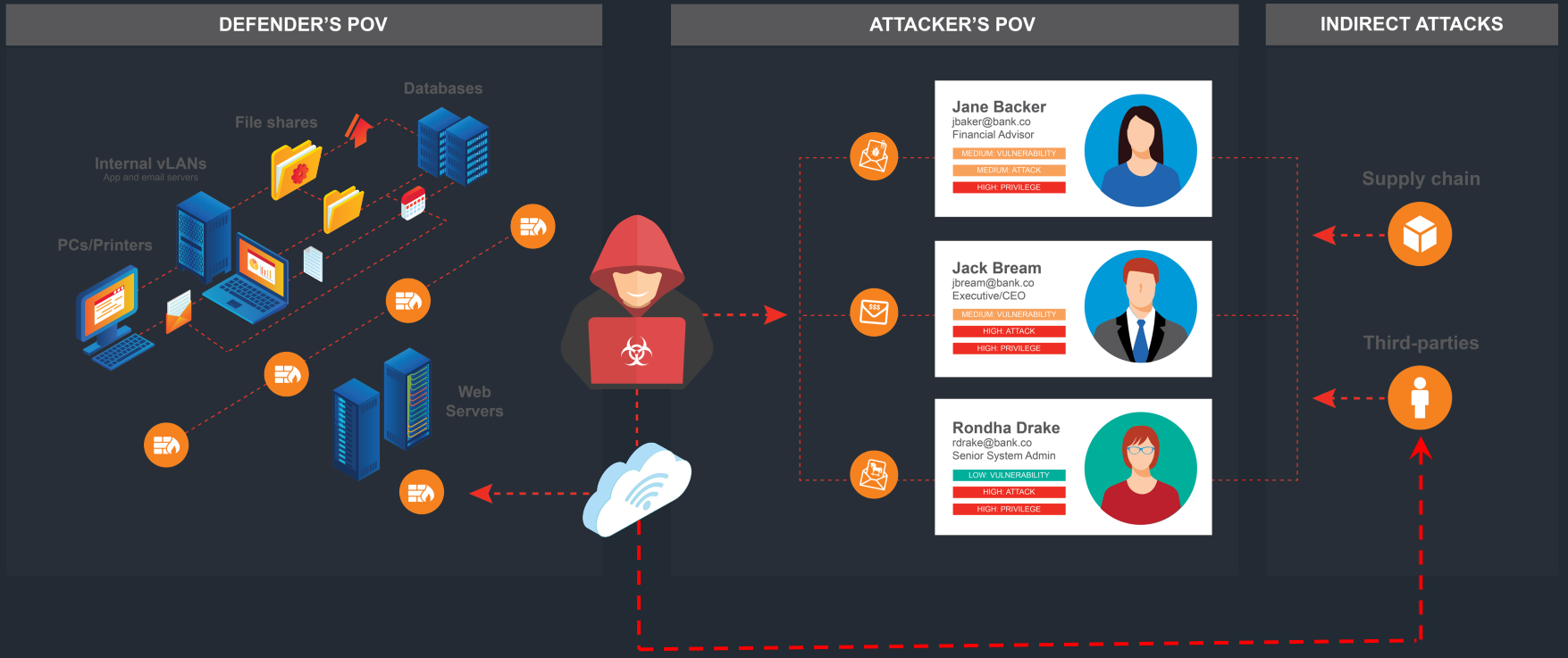


…and more credential phishing.



The human has always been the perimeter.

But have we changed our focus?



People the common link across attack chain

Recon | Initial compromise | Persistence | Info gathering | Priv Esc | Lateral movement | Staging | Impact

- Prevent + detect to identity deception
- Prevent + detect + respond to targeted attacks
- Detect + respond to cloud account takeover

- Prevent common attack paths
- Detect + respond to lateral movement
- Detect + respond to privilege escalation

- Prevent + detect + respond to data exfiltration attempts
- Prevent + detect + respond to domain admin access
- Gain insight into risky user behaviour

Proofpoint **Aegis**

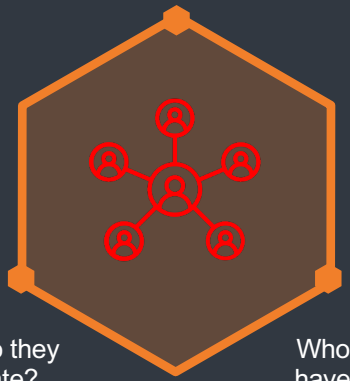
Proofpoint **Identity Threat Detection + Response**

Proofpoint **Sigma**

Answering the questions that matter most

AXIS:
Adversaries

Who are they and what do they want?



How do they operate?

Who else have they attacked?

AXIS:
People

Who is attacked?

Who is risky?

Who has privilege?

AXIS:
Data

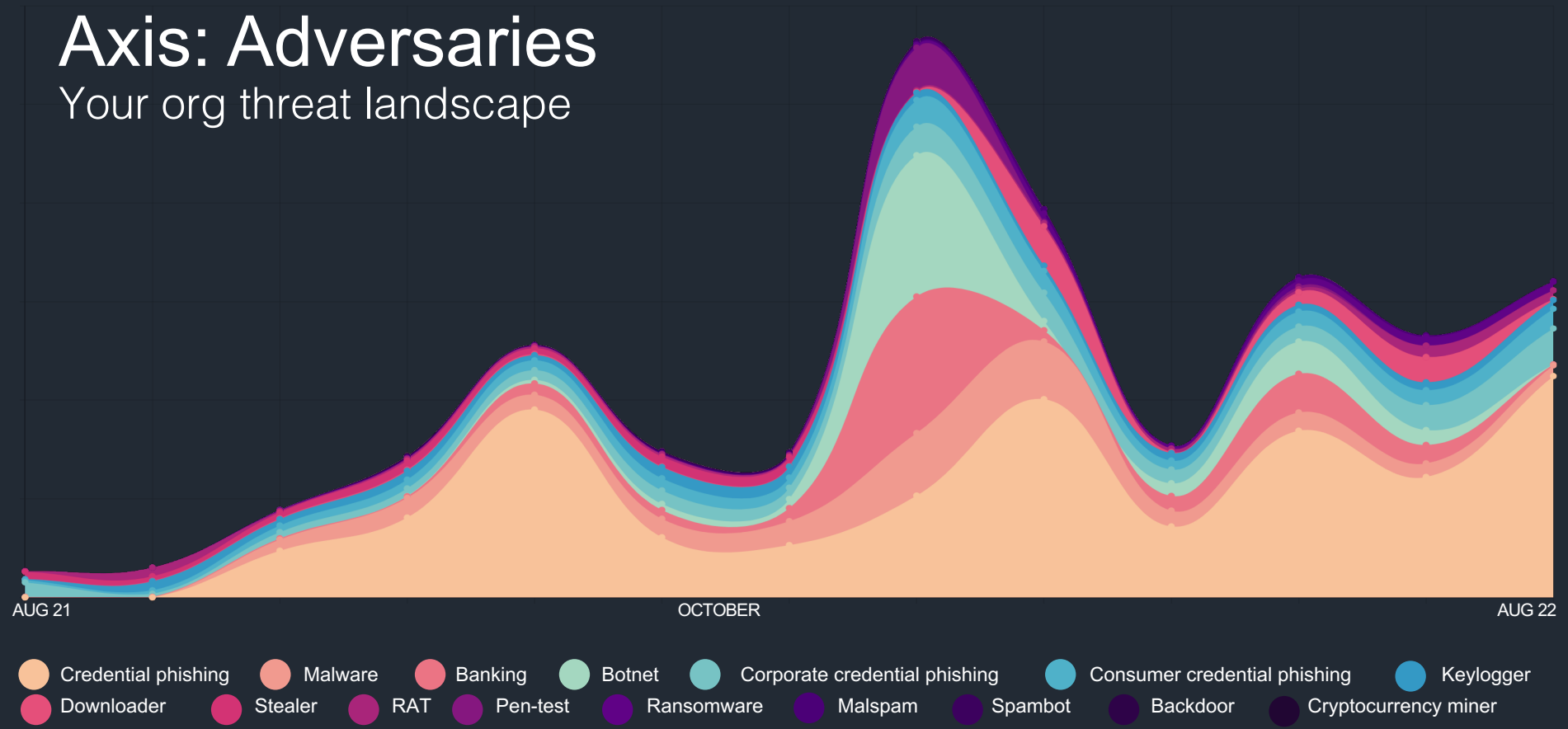
Who has access?

Is it sensitive?

Is it moving or stored in a risky way?

Axis: Adversaries

Your org threat landscape



Axis: People

People are different.... but targetable

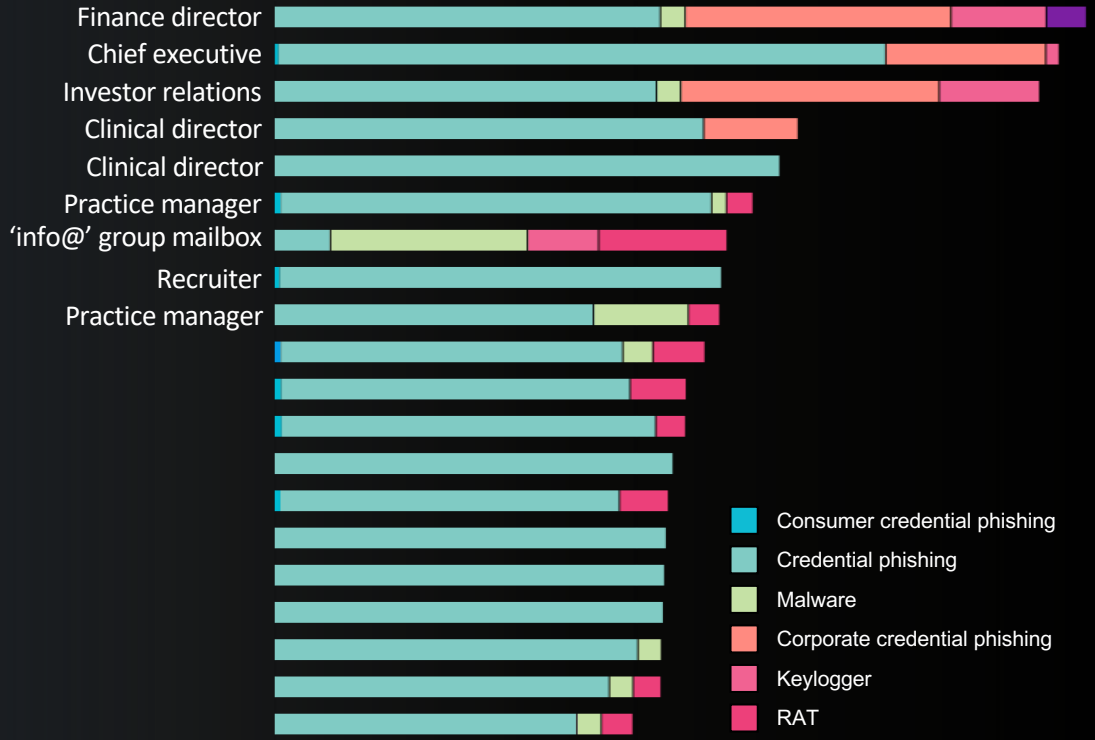
ROLE:

Finance

Targeted with cred phish and RATs

Interacts with risky suppliers

Can move money



Axis: People & Data

Assess the human attack surface

PROBABILITY

Who gets targeted by serious threats? Receive highly targeted, very sophisticated, or high volumes of attacks

LIKELIHOOD

Who is likely to fall for those threats? Clicks on malicious content, fails awareness training, or uses risky devices or cloud services

IMPACT

Who has access to sensitive information? Can access critical systems or sensitive data, or can be a vector for lateral movement

proofpoint.

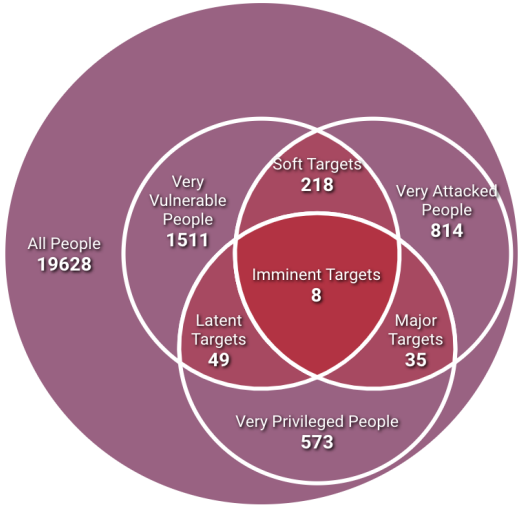
Acme

DASHBOARD

Risk for date: 8/17/2020

Last Calculation of Risk: 8/16/20, 5:40 PM

ALL PEOPLE | IMMINENT TARGETS | MAJOR TARGETS | LATENT TARGETS | SOFT TARGETS | VERY ATTACKED PEOPLE | VERY VULNERABLE PEOPLE



4.2 Risk Level | Risk Motion | Attacked | Privileged | Vulnerable

Description

All employees of the organization including members of Very Attacked , Very Privileged and Very Vulnerable groups as well as all other people.

Overview | New Comers | Seniority | Business Function | Speci

19628 TOTAL

Top Targets

Rank	Name	VIP	Risk
1	Carmine Bowman Payroll Services Senior HR Generalist		6.6
2	Ieystn Mcintosh Service Specialist		6.2
3	Ilona Mann Service Specialist		6.2
4	Demetre Higgins Sr Service Partner - GROUP Service		6.2
5	Manfred Hudson Service Partner - GROUP Service		6.2
6	Janeva Morrison Client Services Supervisor (CSS)		6
7	Raman Dalton Service Representative		6

Adaptive controls that protect people

ROLE:
Finance

Block impostor attacks with ML

Flag risky suppliers with tags

Train on BEC threats

ROLE:
Research Scientist

Web isolation to preserve privacy

Protect cloud collaboration with web, endpoint DLP

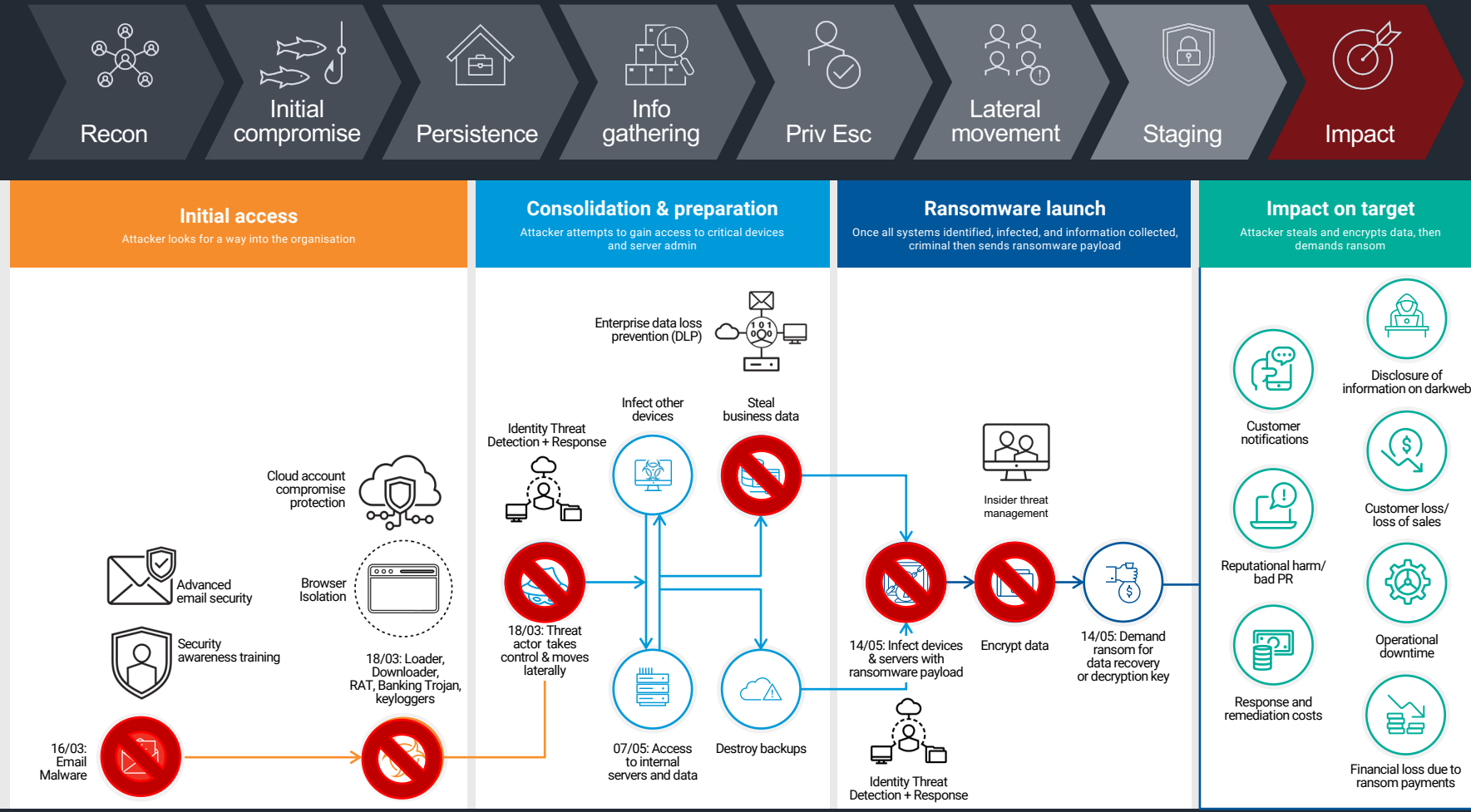
Deliver custom training on campaigns targeting intellectual property

ROLE:
Support

Isolate all links to shared alias so clicks do no harm

Use ITM to protect customer data

Train on data handling



Protect people by blocking threats from reaching users and by training them.
Education is more effective when it's:

- Individualised,
- Context specific and
- Delivered at a time, and in a way, the user prefers

Knowledge of who is being attacked, and with what, provides actionable intelligence to:

- Protect the individual & enterprise
- Drive user engagement
- Assess the threat actor goals

People Risk – Bring these together to **allow a risk-based approach**

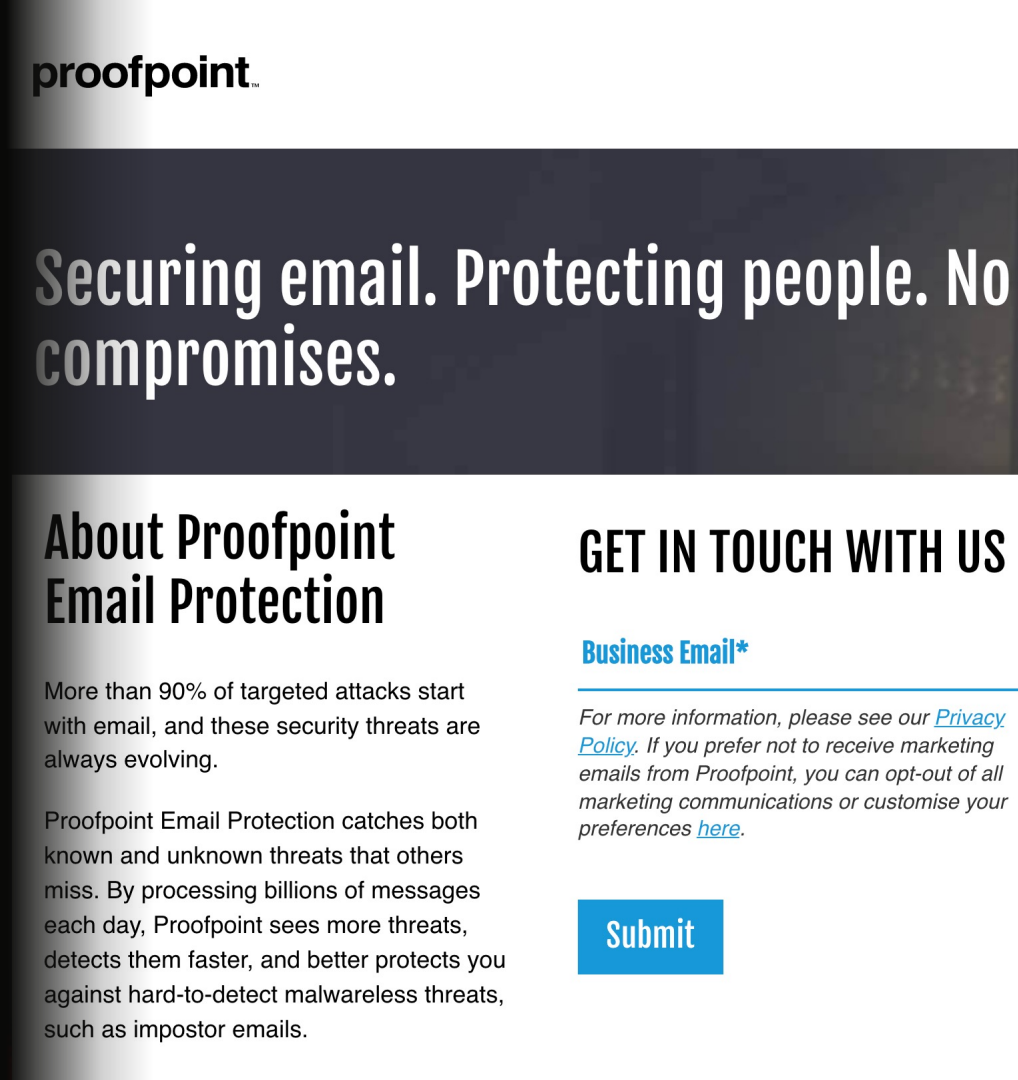
- Automated, dynamic controls
- Personalised messaging & education
- Insightful Board level metrics

proofpoint.

Learn more

Uncover your Very Attacked People

go.proofpoint.com/en-email-security-get-in-touch.html



proofpoint®