Protecting people, together

Werner Thalmeier
VP, EMEA Systems Engineering

BKA - Cybercrime Bundeslagebild 2021

Schaden durch:	Schadens-summen in Mrd. Euro (2021)	Schadens-summen in Mrd. Euro (2019)	Schadens-summen in Mrd. Euro (2017)	Schadens-summen in Mrd. Euro (2015)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	61,9	13,5	5,3	7,2
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	**24,3**	**5,3**	**0,7**	**1,5**
Datenschutzrechtlich[illegible]nen (z.B. [illegible] von K[illegible])	17,1	[illegible]	3,2	2,0
Patentrechtsverletzungen (auc[illegible]chon vor der Anm[illegible]lung)	30,5	14,3	7,7	9,4
Umsatzeinbußen durch Verlu[illegible]on Wettbewerbs[illegible]teilen	29,0	[illegible]	8,6	6,4
Umsatzeinbußen durch n[illegible]gemachte Produk[illegible](Plagiate)	22,7	11,1	3,5	11,5
Imageschaden bei Ku[illegible]n oder Lieferant[illegible]Negative Medienberichterst[illegible]ung	12,3	9,3	7,7	5,9
Kosten für Ermittlungen und Ersatzmaßnahmen	13,[illegible]	[illegible]	10,6	-
Kosten für Rechtsstreitigkeiten	12,[illegible]	15,6	5,5	6,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	2,2	0,9
Sonstige Schäden	0	< 0,1	< 0,1	0,1
Gesamtschaden pro Jahr	**223,5**	**102,9**	**54,8**	**51,2**

Abbildung 29: Verursachte Schäden durch Cybercrime. Quelle: Die Einzelzahlen sowie Summenwerte wurden in dieser Form von Bitkom e.V. aus dem Wirtschaftsschutzbericht 2021 (veröffentlicht am 05.08.2021) übernommen.

223,5

© 2022 Proofpoint. All rights reserved

Quelle: BKA Cybercrime Bundeslagebild 2021

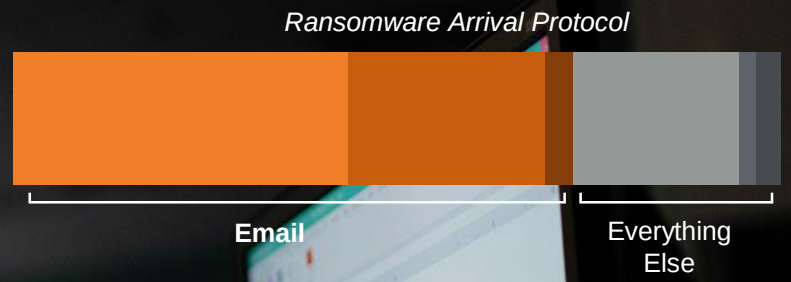
DESPITE ALL THE CHANGE IN MEGATRENDS, ONE CONSTANT IN CYBERSECURITY

	2012	2017	2022
MEGATREND	Mobility/BYOD	Cloud	Work from anywhere
DOMINANT CYBER RISKS	Data breaches, payment card theft, espionage, compliance	Automated ransomware, banking trojans	Big game ransomware, BEC, leavers taking data
BIGGEST RISK	**PEOPLE** "Most major cyberattacks on U.S. corporations use social engineering" The Washington Post	**PEOPLE** 94% of malware comes via email, phishing involved in most breaches verizon DBIR	**PEOPLE** 85% involved a human element, just 3% involved a technical vulnerability verizon DBIR

TOP 3 CYBERSECURITY RISKS: ALL PEOPLE-CENTRIC

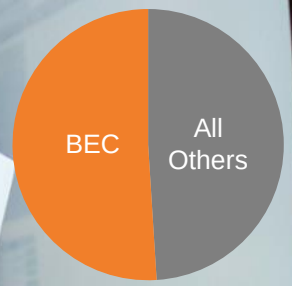
Vast majority of ransomware attacks start with email

— paloalto NETWORKS research



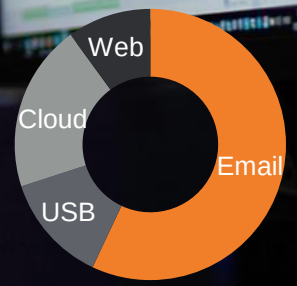
BEC losses exceed all other cybersecurity losses combined

— data for 791,790 incidents



99% of data loss incidents are human-driven

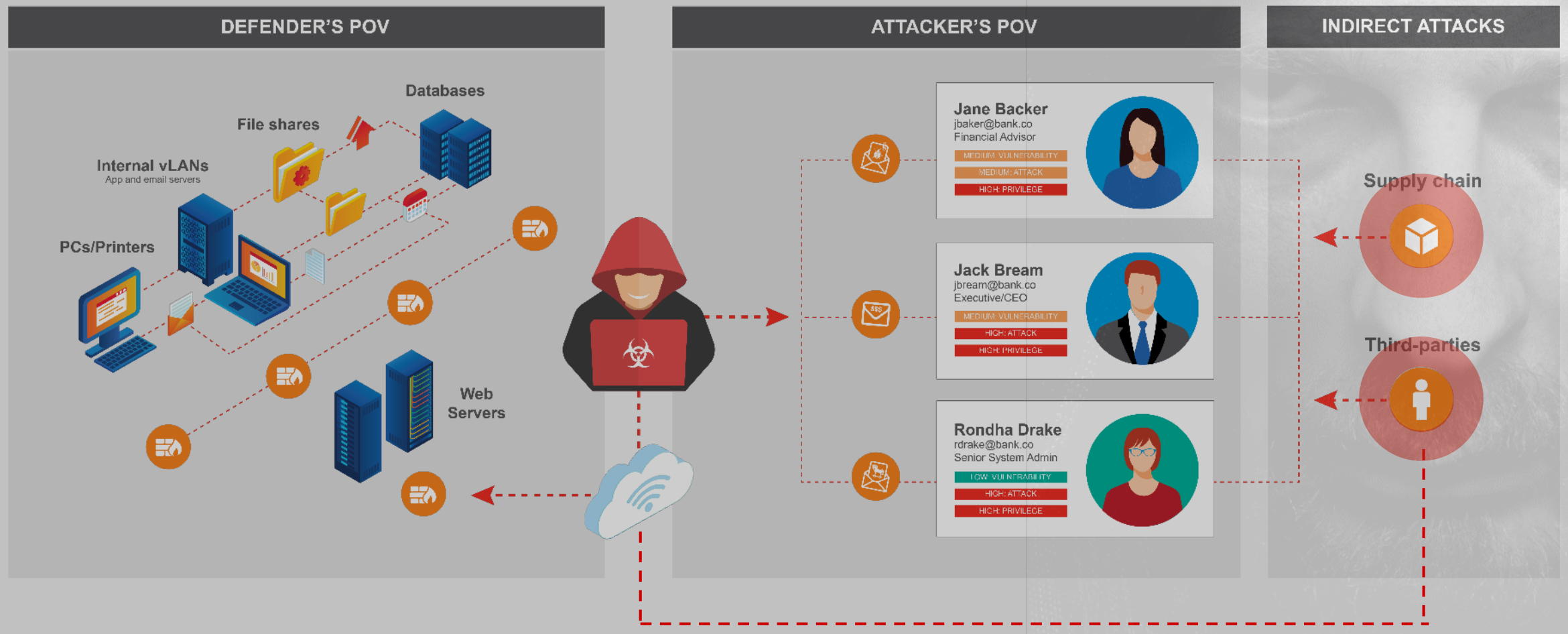
— proofpoint data across 3,000 organizations



85%

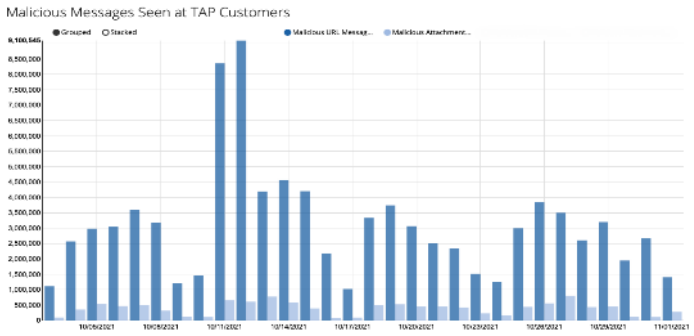
INVOLVED A HUMAN ELEMENT

The Attackers Point of View



Modern Threat Landscape

Identity Theft



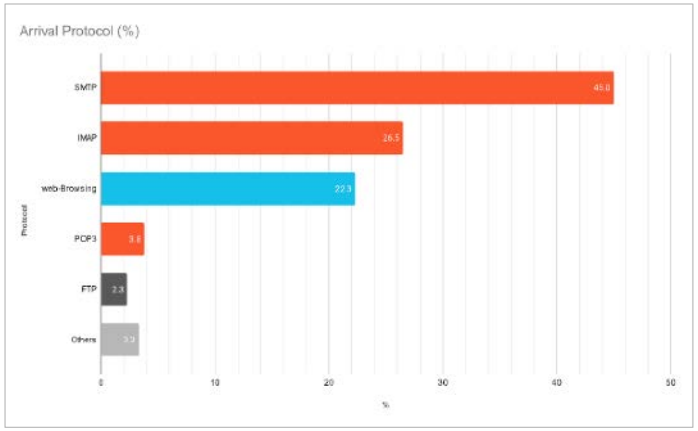
Evilginx2

Modlishka

Evolution of Identity Theft

- **Credential harvesting**
- **Human Interactive attacks**
- **MFA attacks**

Ransomware

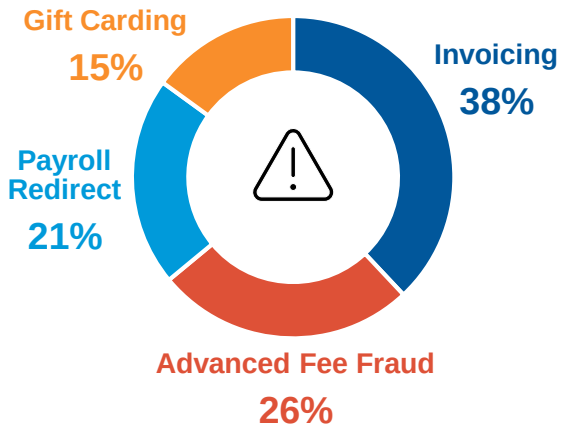


Evolution of Ransomware

- **Single Stage**
  - Loki
  - WannaCry
- **Multi-stage**
  - IcedID-> **MAZE**
  - NimzaLoader->**Cobalt**
  - BazaLoader→**Ryuk**
- **Text based**
  - **TOAD**
  - **Insider**
  - **Targeting**

BEC

BEC Landscape



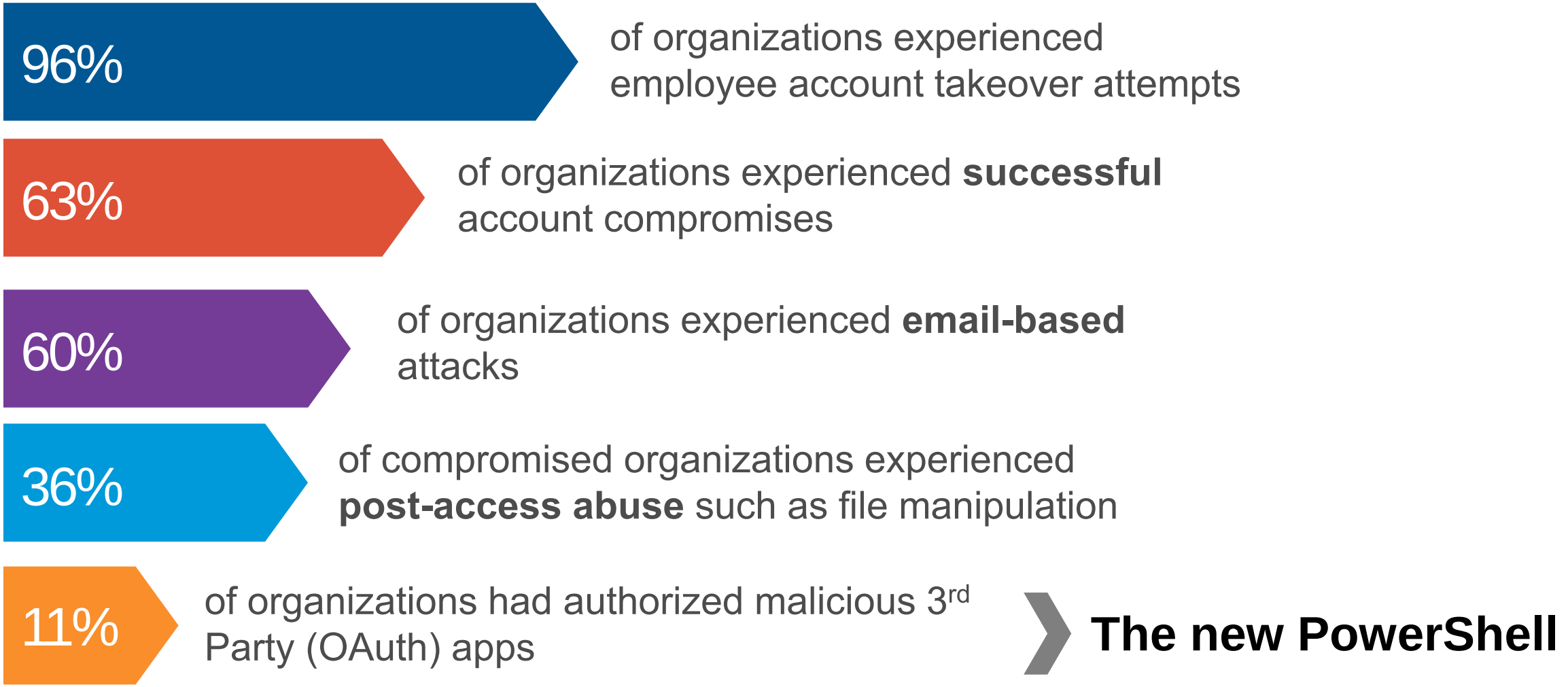
Evolution of BEC

- **Direct Domain**
- **Lookalike & freemail**
- **Supplier lookalike & Compromise**

Targeted Attacks at Scale

proofpoint.

Cloud Threats Driving Majority of Email Based Attacks



Based on data from 2200+ monitored Cloud environments – last 6 months

proofpoint.

The Infection Chain - Nemty

Phishing Email

Link to
Zip File
Download

Zip File

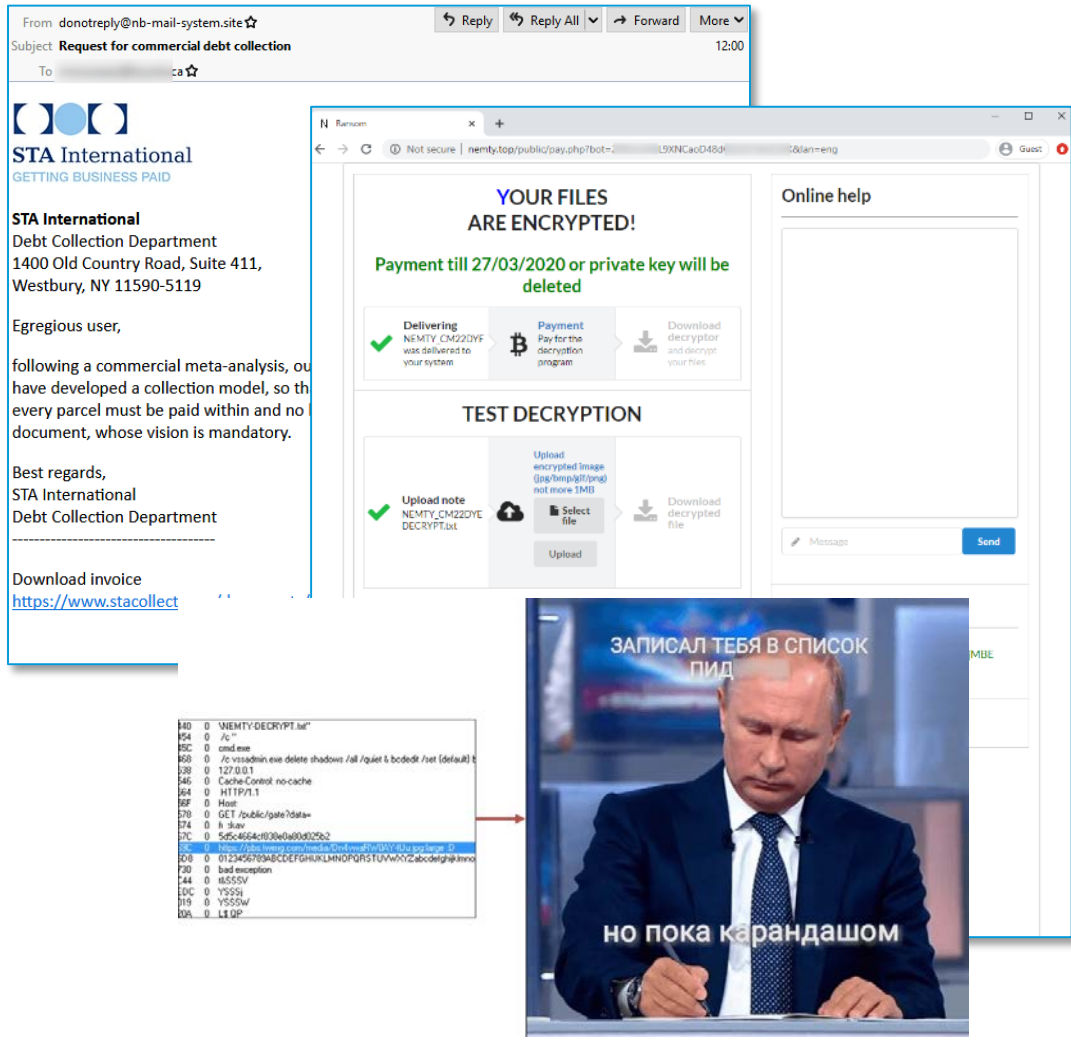
.lnk executable

Nemty

proofpoint.

Debt Collection Lures and Ransomware

- Emails received with STA Tax Collection lures and a link to download a zip file.
  - Zip file contained a .lnk executable that would then utilize Powershell to download and execute the Nemty Ransomware
- **Medium Sized Campaign:**
  - Targets:
    - More than 1,000 messages
    - More than 100 customers targeted primarily in Canada
    - All verticals targeted but the Healthcare vertical was targeted more than the rest.
- **Impact:** Denial of Service
  - Nemty is a standard ransomware that scans the infected system's file system for files using specific file extensions and then encrypts them. Once the process is done, the decryption of the files is then ransomed to the end user for a monetary payment.



proofpoint.

Anatomy of the ransomware attack

Detection takes too long

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

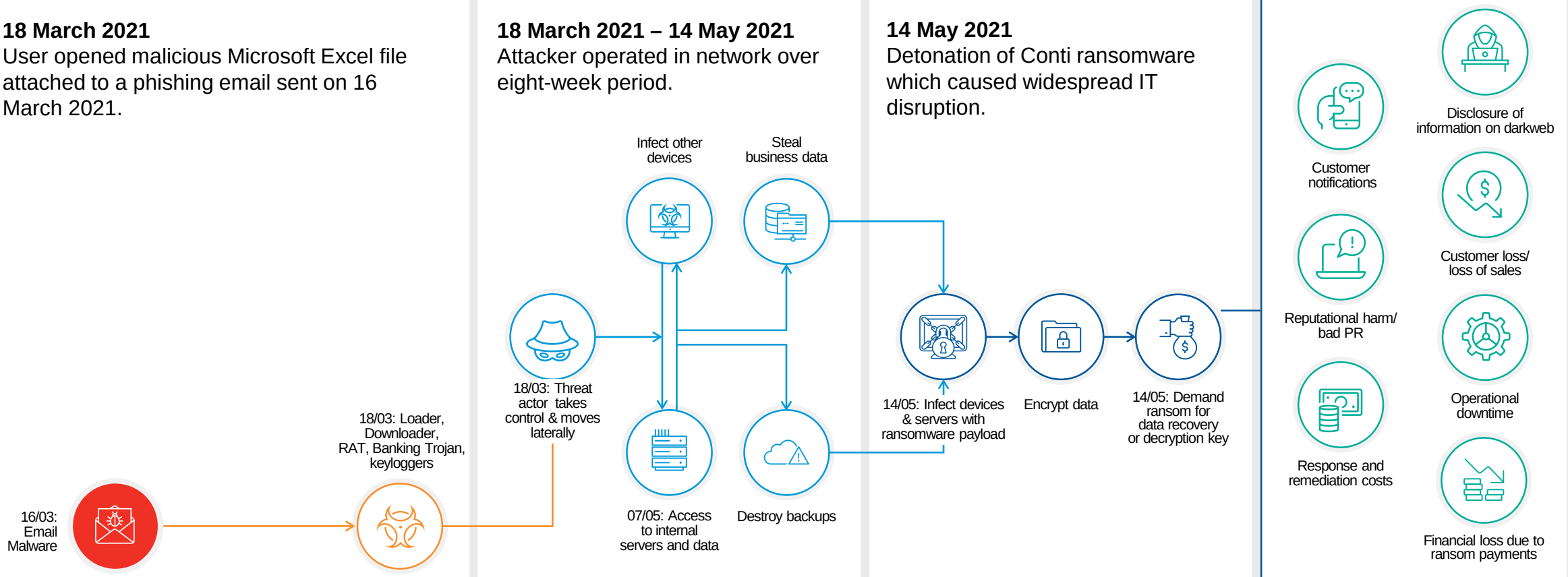
Once all systems identified, infected, and information collected, criminal then sends ransomware payload

14 May 2021

Detonation of Conti ransomware which caused widespread IT disruption.

Impact on target

Attacker steals and encrypts data, then demands ransom



© 2022 Proofpoint. All rights reserved. | Proofpoint, Inc. – Confidential and Proprietary

BKA - Cybercrime Bundeslagebild 2021

Phishing ist und bleibt einer der beliebtesten Eintrittsvektoren. Die verwendeten Narrative sind mannigfaltig und passen sich dem aktuellen politischen wie gesellschaftlichen Geschehen an.

Abbildung 11: Anzahl der durch die Anti-Phishing-Working-Group festgestellten Phishing-Seiten seit 2019. Die orangene Linie zeigt den Durchschnitt im betrachteten Zeitraum, die rote Linie gibt den Tendenzverlauf an.

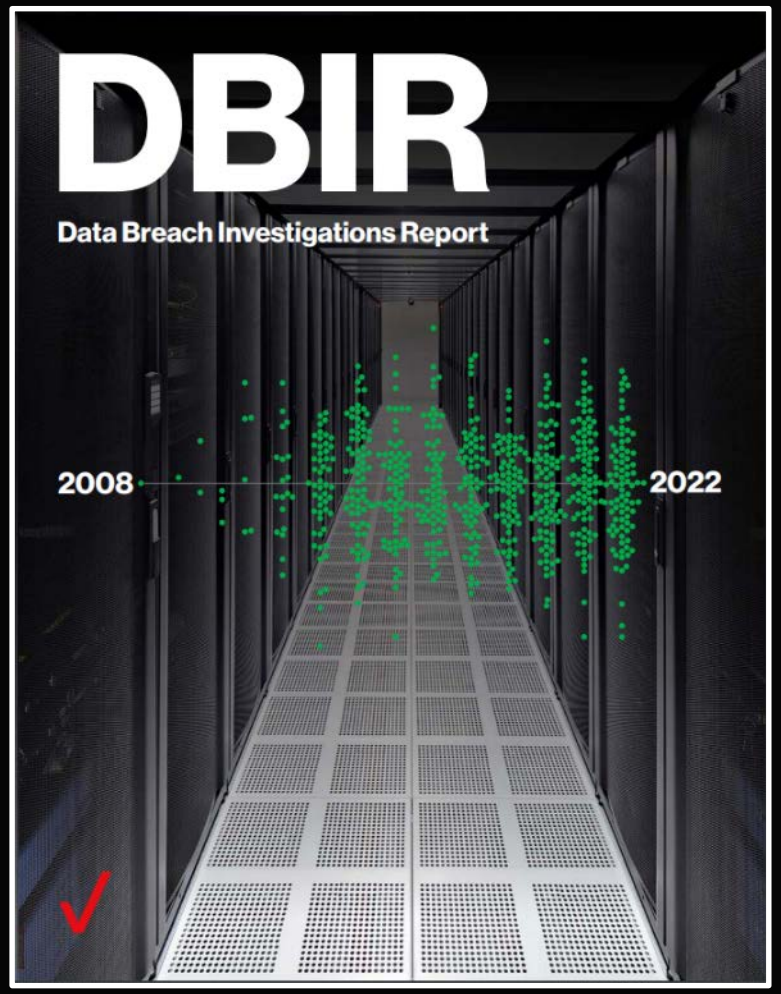
© 2022 Proofpoint. All rights reserved

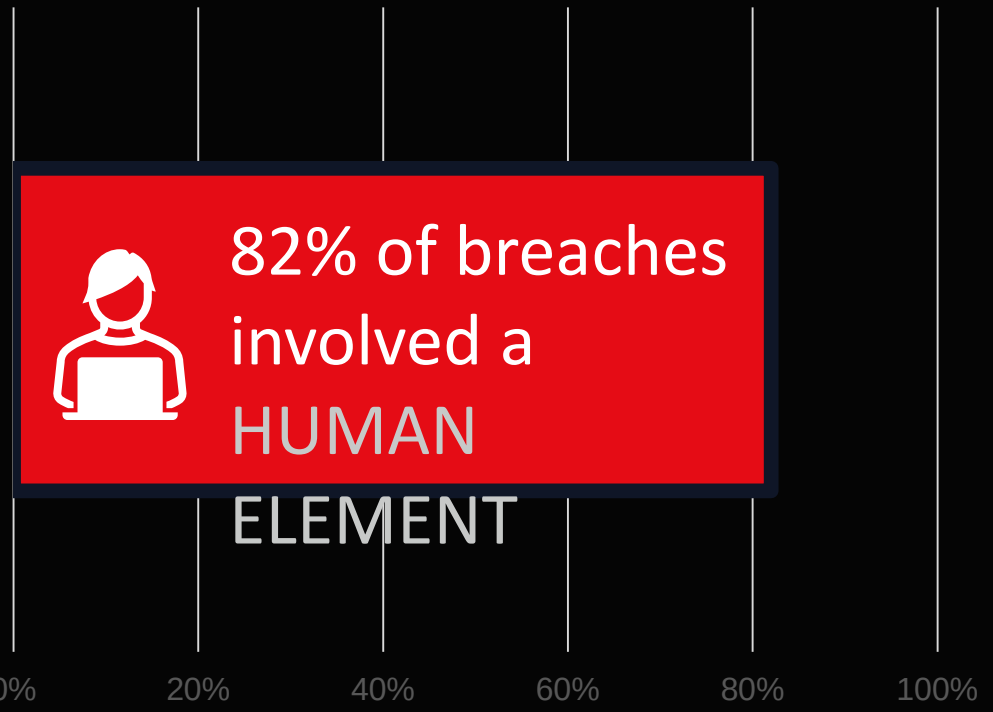
Quelle: BKA Cybercrime Bundeslagebild 2021

“Only amateurs attack machines, professionals target people.”

Bruce Schneier
https://www.schneier.com/blog/archives/2013/03/phishing_has_go.html

Verizon DBIR 2022





… almost half of breaches involve CREDENTIALS
… ~1 in 5 Breaches involve INSIDER THREATS

proofpoint.
© 2022 Proofpoint. All rights reserved. | Proofpoint, Inc. – Confidential and Proprietary

THE HUMAN ATTACK SURFACE. WHO ARE YOUR VAPS™?

VERY ATTACKED PEOPLE

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

VERY VULNERABLE PEOPLE

Who is likely to fall for those threats? They click on malicious content, fail awareness training or use risky devices or cloud services.

VERY PRIVILEGED PEOPLE

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

PEOPLE ARE COMPLEX, DIFFERENT

ROLE:

Finance

VAP

Interacts with risky suppliers

Can move money

ROLE:

Research Scientist

Fully remote

Part of works council

Collaborates externally via cloud apps

ROLE:

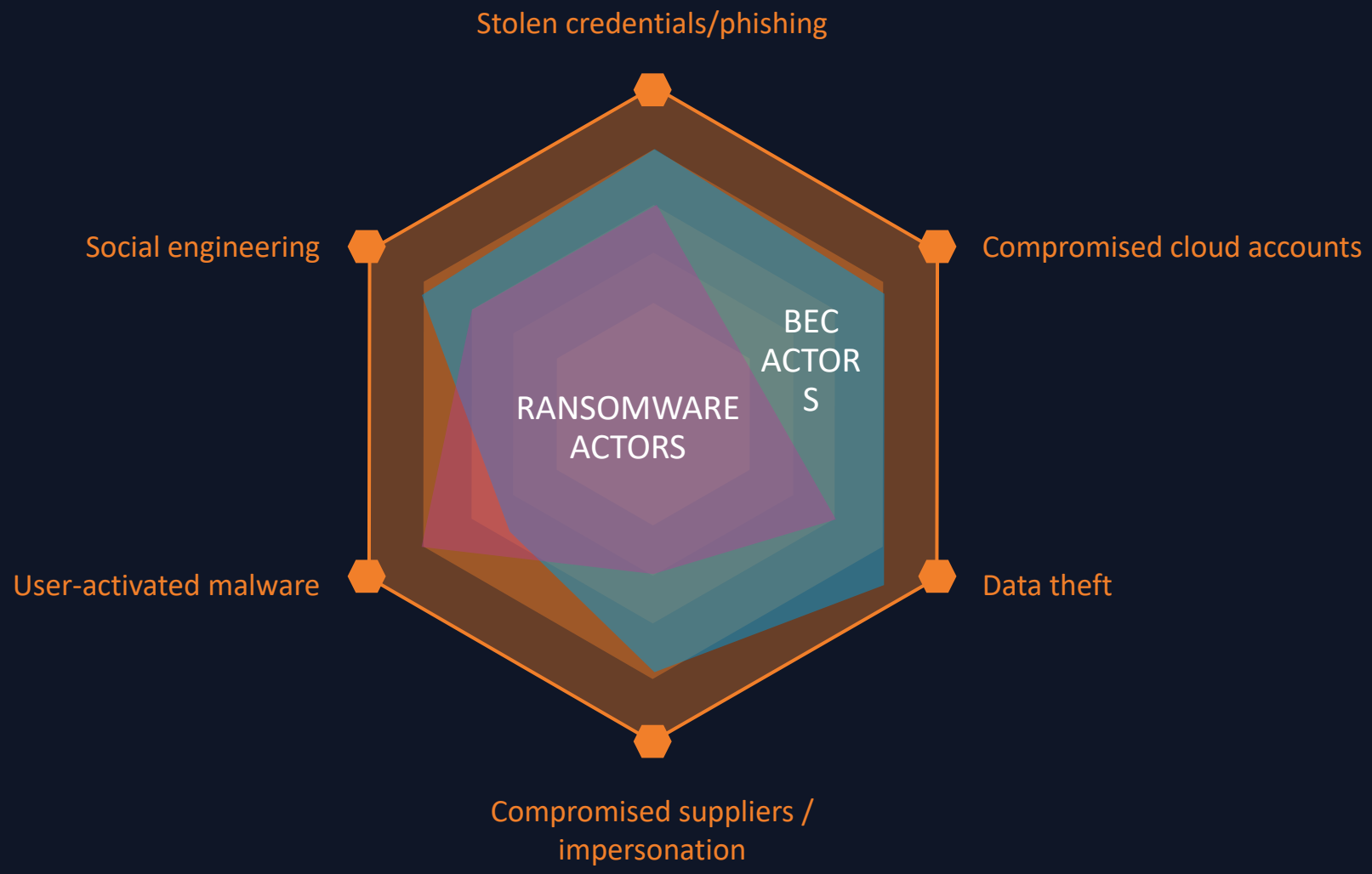
Support Contractor

Targeted via alias

Clicks everything

Handles customer data

THE ATTACKER'S PLATFORM FOR PEOPLE-CENTRIC EXPLOITATION



PROTECTION FOR PEOPLE, HOW AND WHERE THEY NEED IT

ROLE:

Finance

Block impostor attacks with ML

Flag risky suppliers with tags

Train on BEC threats

ROLE:

Research Scientist

Web isolation to preserve privacy

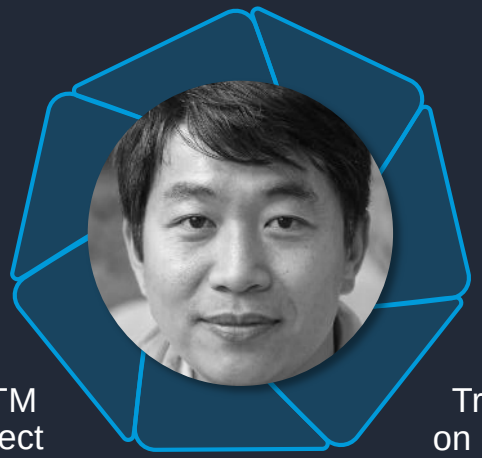
Protect cloud collaboration with web, endpoint DLP

Deliver custom training on campaigns targeting intellectual property

ROLE:

Support

Isolate all links to shared alias so clicks do no harm



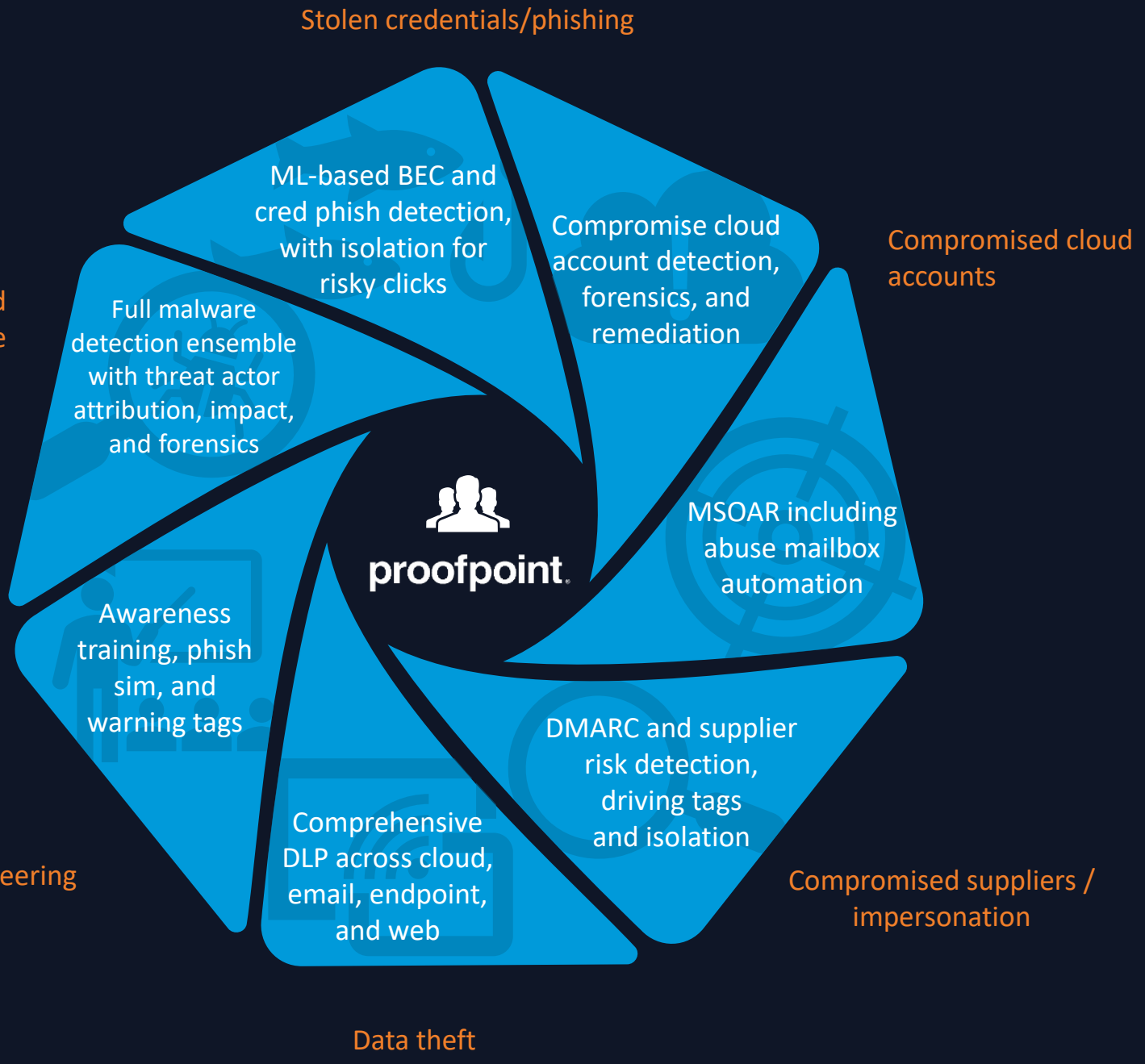
Use ITM to protect customer data

Train on data handling

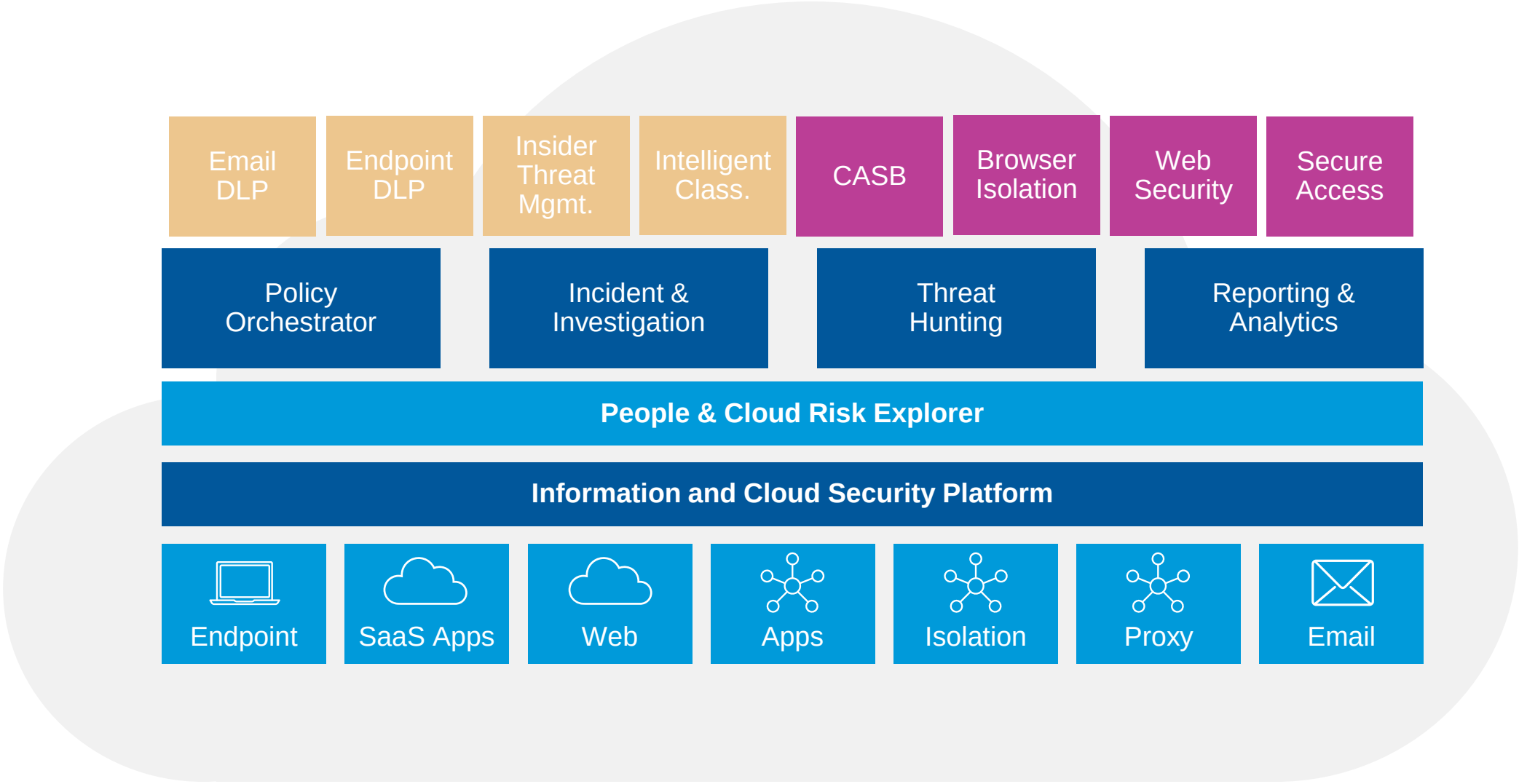
PLATFORM APPROACH: THE RIGHT PROTECTION FOR THE RIGHT PEOPLE

“The evolution in threats has led to increased demand for other techniques and services, such as DMARC, cloud access security broker (CASB)/API integrations, continuous awareness and mail-focused security orchestration, automation and response (MSOAR).”

Gartner®



Bring it All Together With One Platform



proofpoint.

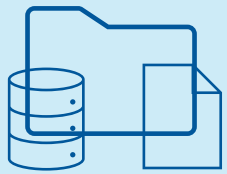
Our mission: Protect people \ Defend data

Protect People:

- Email Security and Fraud Defense
- Cloud Security
- Security Awareness

Defend Data:

- Data Loss Prevention
- Insider Threat
- Intelligent Compliance



Shared Intelligence Graph

Unified People-Centric Risk Visibility

Applied Machine Learning

proofpoint.

© 2021 Proofpoint. All rights reserved. | Proofpoint, Inc. – Confidential and Proprietary