proofpoint®

5 mars 2019

FACTEUR HUMAIN / PAYSAGE des MENACES CYBER 2018

Laura Peytavin
Senior Sales Engineer South EMEA
lpeytavin@proofpoint.com

LES MENACES

La perception

La réalité à partir de données massives

proofpoint.

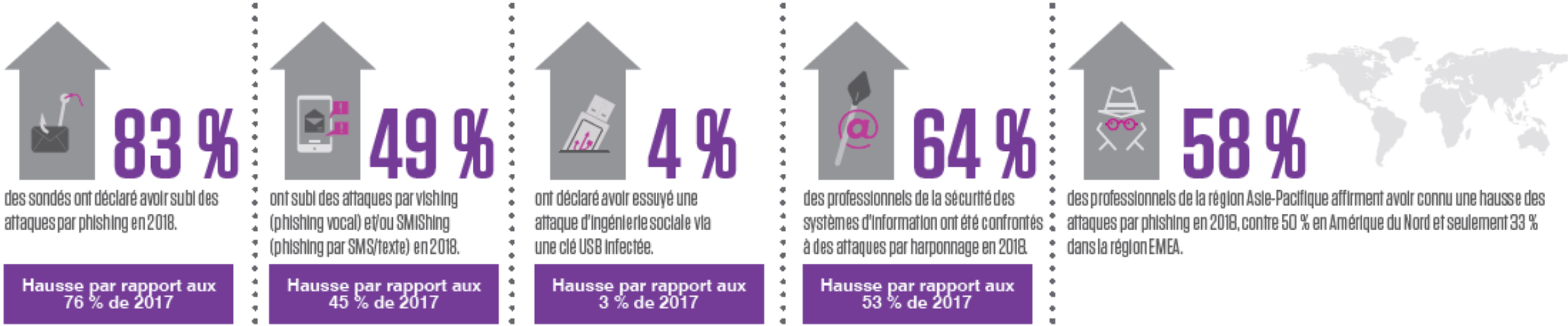
Le premier vecteur d’attaque en volume est toujours…

Source: 2018 Verizon DBIR

Ce que constatent les personnels en charge de la cybersécurité des entreprises

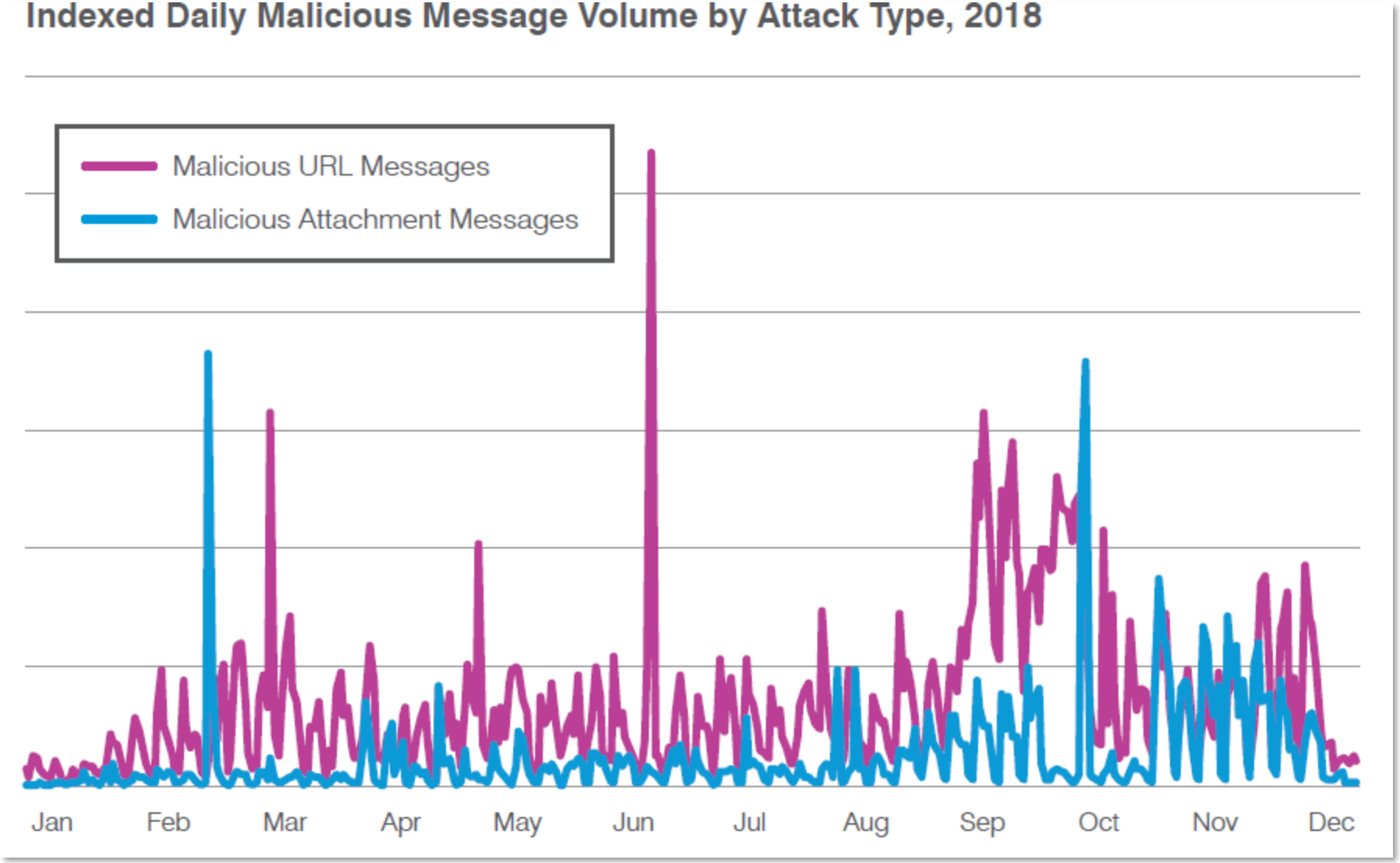
(ENQUÊTE WOMBAT / REPORT OF THE PHISH 2019)

- Analyse sur 15000 retours d'enquête sur les clients Proofpoint/Wombat
- Ainsi qu'une enquête sur plus de 7000 personnes majeures en poste (US, UK, FR, GER, IT, AUS,JP)



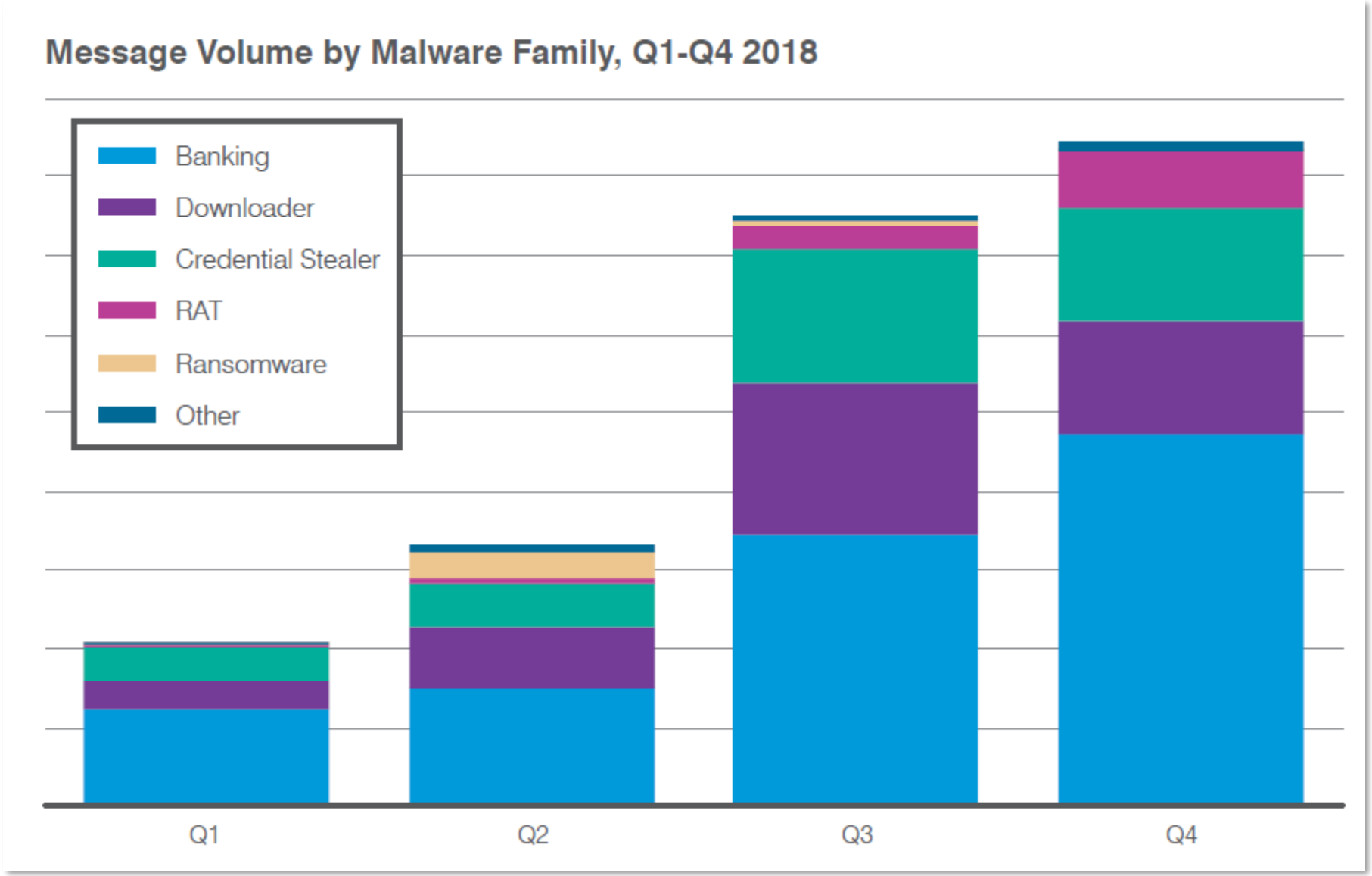
proofpoint.

Attaques par URL ou pièces jointes – récap sur 2018



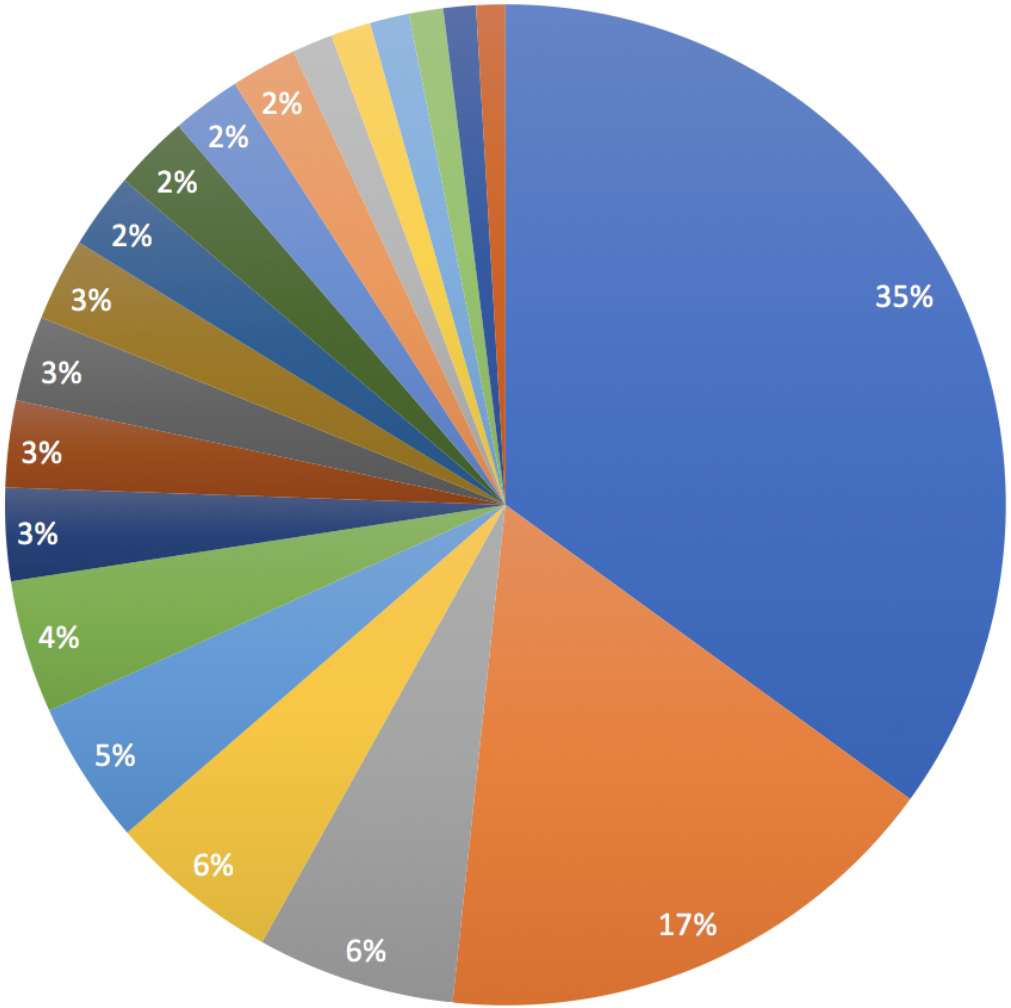
proofpoint.

Distribution des malwares sur 2018



proofpoint.

Représentation des différents template de phishing

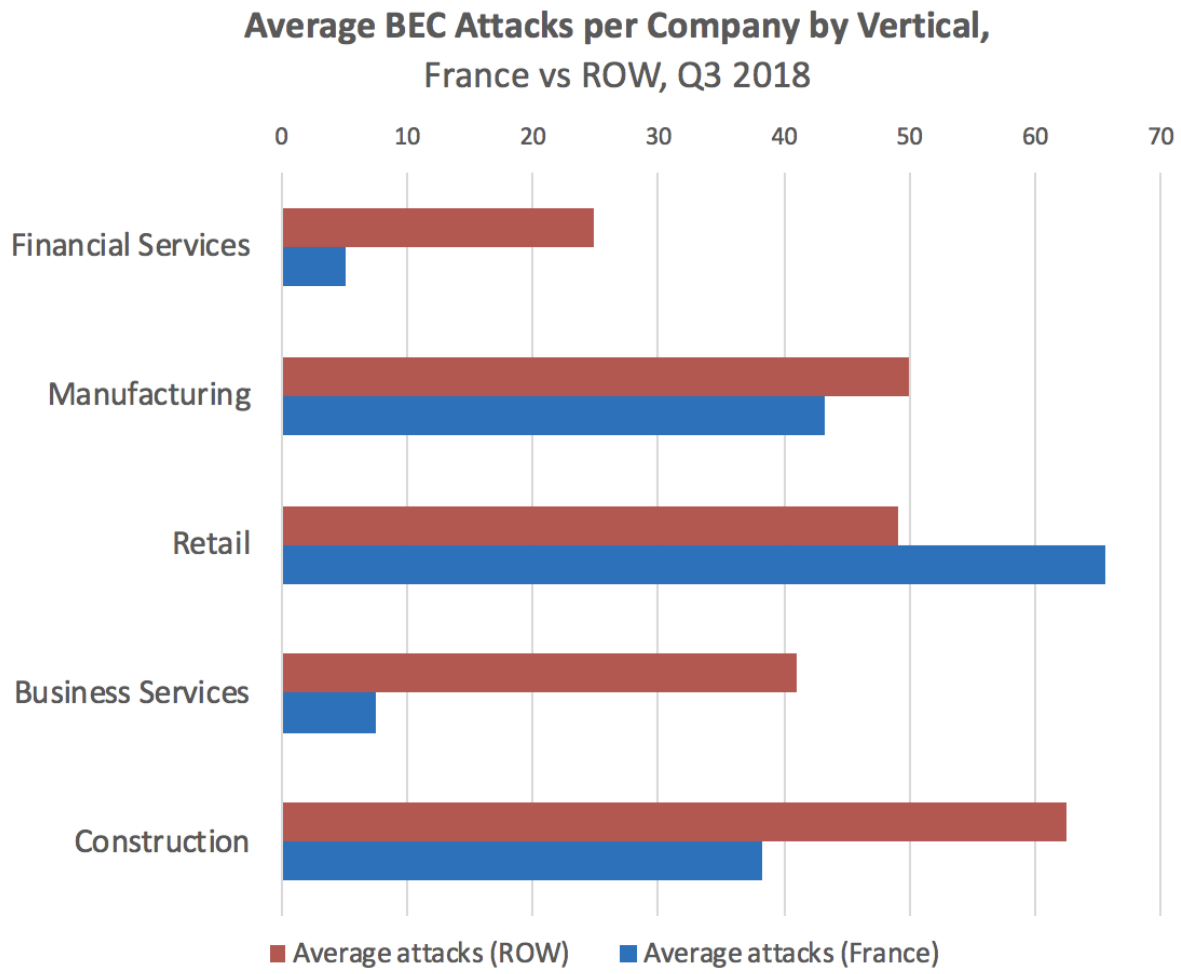


- Generic Email Credential Harvesting
- Financial Institution Phishing
- Office 365 Account Phishing
- Microsoft OWA Phishing
- Adobe Account Phishing
- Google Drive Phishing
- Linkedin Account Phishing
- OneDrive Phishing
- Windows Settings Phishing
- Interac Phishing
- Postal / Shipping Company Phishing
- Netflix Phishing
- Microsoft Excel Online Phishing
- cPanel Phishing
- Yahoo Email Account Phishing
- Secure Cloud File Phishing
- Docusign Phishing
- Dropbox Account Phishing
- Flazio Hosted Credential Harvesting
- Microsoft Online Document Phishing

proofpoint.

Arnaques au président

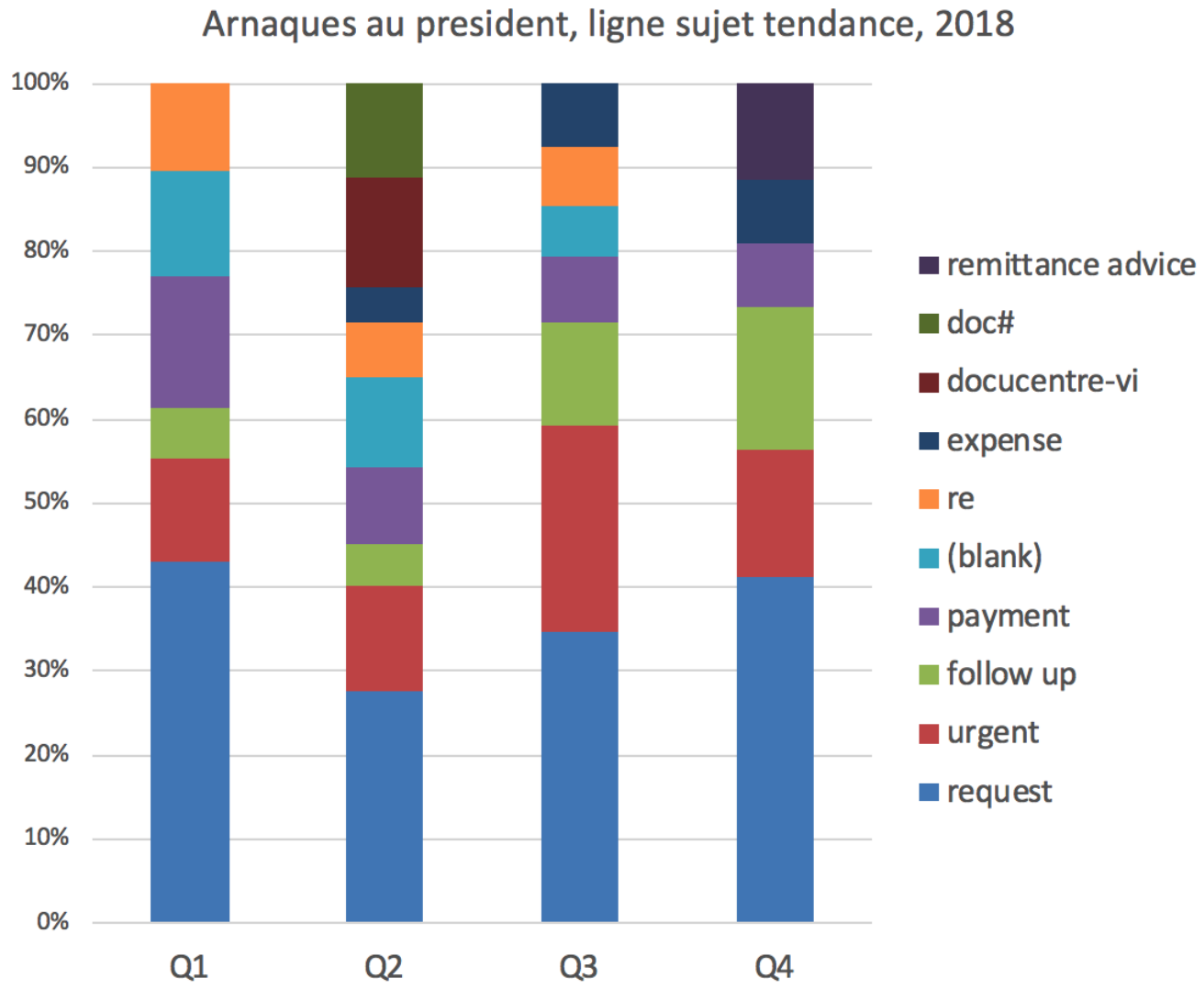
- Les sociétés Française ont reçu en moyenne 28 email BEC en Q3 2018
  - Moins que les 37 messages de moyenne dans le reste du monde
- Comparaisons concernant ces attaques avec le reste du monde
  - On constate globalement l'utilisation des mêmes techniques de façon globale.
  - La technique la plus populaire est de créer un compte email gratuit et modifier le *display name* en utilisant le nom d'un exécutif de la société ciblée. Le service le plus utilisé par les attaquants est *gmail*, en France comme aux Etats Unis.
- Pas forcement après le « coup du siècle »



proofpoint.

Bien choisir son sujet …

- L'anglais est toujours utilisé dans la majorité des sujets bien que ciblant des entreprises Françaises.
- Les sujets les plus utilisés en France sont :
  - *request*
  - *urgent*
  - *payment*
  - *Re :*
- Q4 a vue une augmentation autour du thème des factures



Une tactique qui n’est plus un signal faible : le typosquatting ou homoglyphie IDN

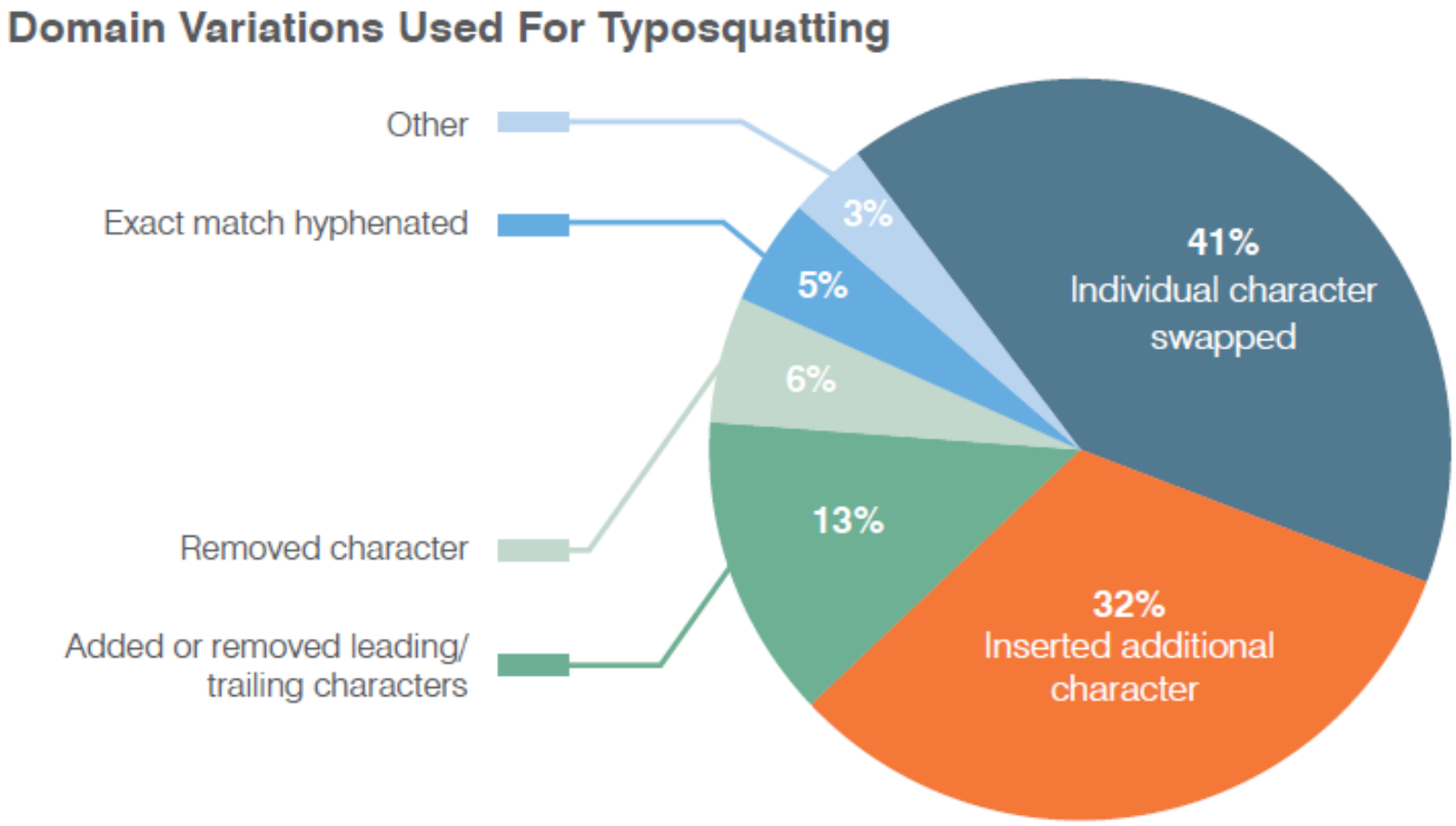
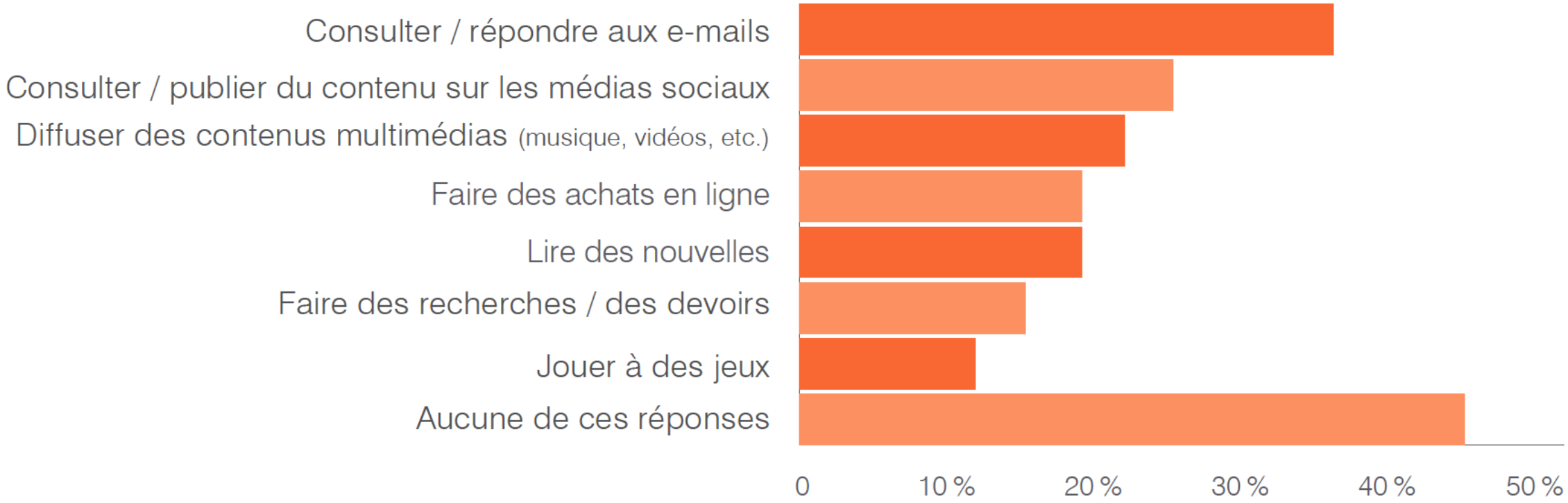


Figure 10: Common variations used in suspicious domain registrations and typosquatting

Le risque s’étend au delà des employés

Quelles activités permettez-vous aux membres de votre famille ou à vos amis de confiance d'effectuer sur l'appareil que vous a fourni votre employeur ? (cochez toutes les réponses pertinentes)



Source: Rapport sur les risques lies aux utilisateurs, Proofpoint Wombat, Octobre 2018

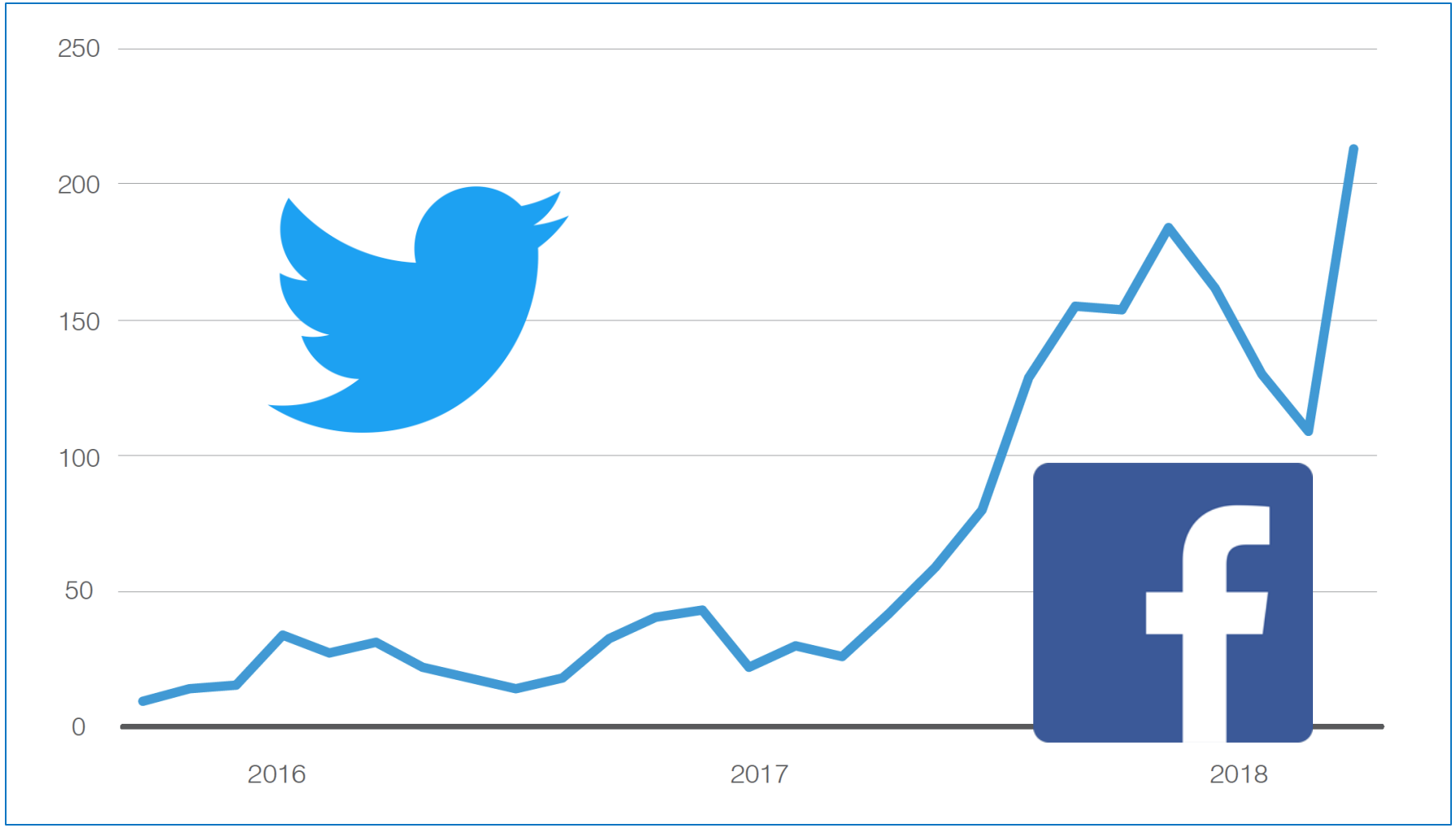
proofpoint.

Réseaux Sociaux : la fraude en plein essor

Social media customer support fraud increased

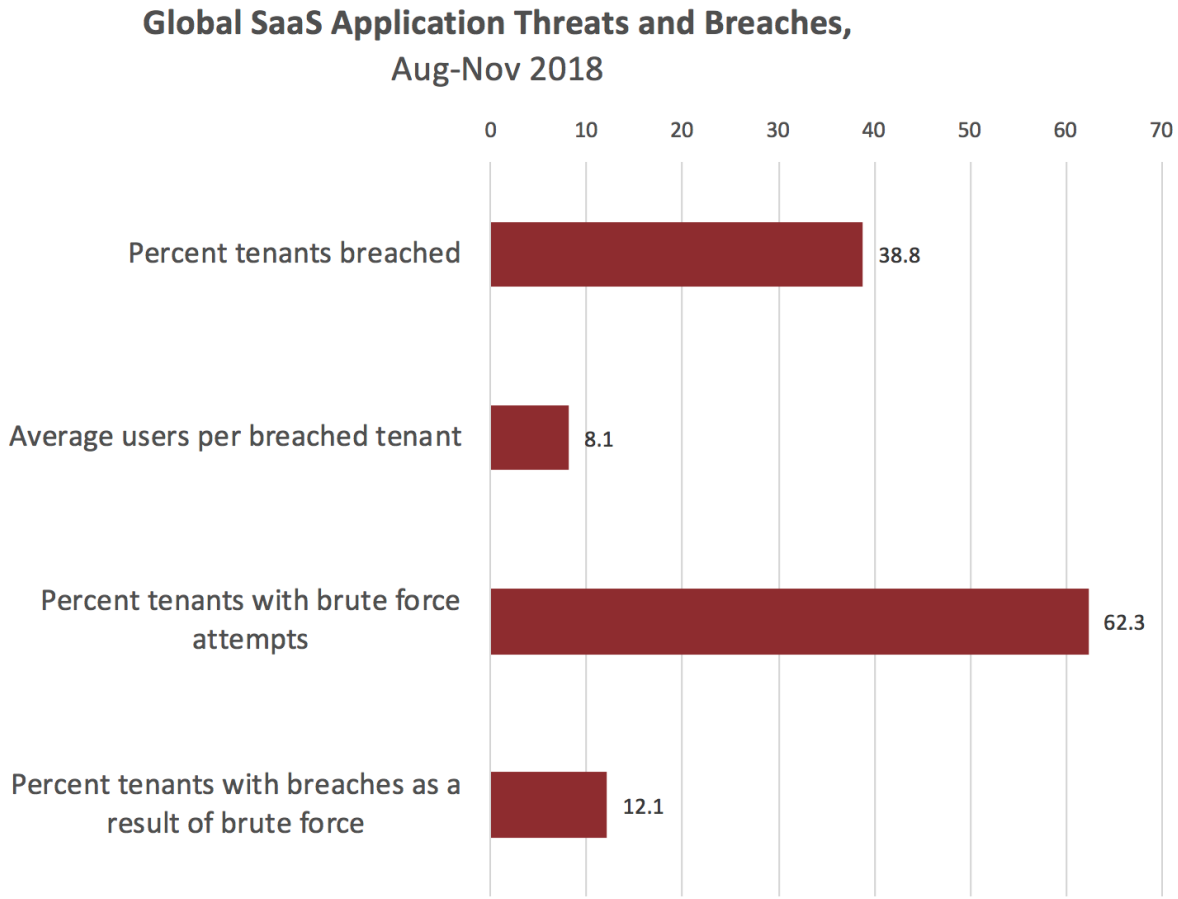
486%

compared to Q3 2017, its highest level ever.



Dans le Cloud, les menaces ciblent directement les personnes

- Les organisations Françaises semblent visiblement plus ciblées et impactées par les attaques
- Moins d'un pourcent des comptes compromis sont des VIP, mais avec conséquences plus importantes.
- Parmi ces connexions suspicieuses, on compte :
  - Des sources malicieuses comme des bots, scanning hosts, sorties de nœud Tor et autres
  - Des « Non-human logins » depuis des infrastructures cloud type AWS/Azure ainsi que des services tiers.
  - Du « Too-fast-to-travel », « Too-fast-to-type »



proofpoint.

Les tactiques d'attaques sur comptes utilisateurs dans le Cloud (O365 / G-Suite)

01 CHASSE AUX IDENTIFIANTS

- Vols d'identifiants* par phishing
- Identifiants revendus, issus de brêches publiques
- Malwares chargés de capturer des identifiants
- Analyse des Réseaux Sociaux
- Chasse aux addresses de courriels

02 INFILTRATION

- "Brute Force"
- Login/connexion

03 EXTENSION & ENCRAGE

Profiter du 1er compte compromis pour lancer des attaques (EAC/BEC)

- Lecture des courriels et du calendrier
- Prise de connaissance des procédures internes
- Déplacement latéral (courriels de phishing pour voler identifiants d'autres comptes)

Encrage de la brêche

- Suppression des notifications par courriel
- Création de règles de transfert de courriel
- Ajout d'App. malicieuse (construites avec accès oAuth)
- Changement des droits de partage
- Création de comptes admin
- Ajout de compte à des groupes d'admin.
- Suppression de la double authentification (2FA)
- Téléchargement et partage de données/documents virusés

04 EXFILTRATION

Monétiser

- Fraude au transfert d'argent

Vol de données

- Export
- Partage
- Transfert

- : identifiant de connexion et mot de passe inclus

BEC : Business Email Compromise

EAC : Email Account Compromise

proofpoint

LE FACTEUR HUMAIN

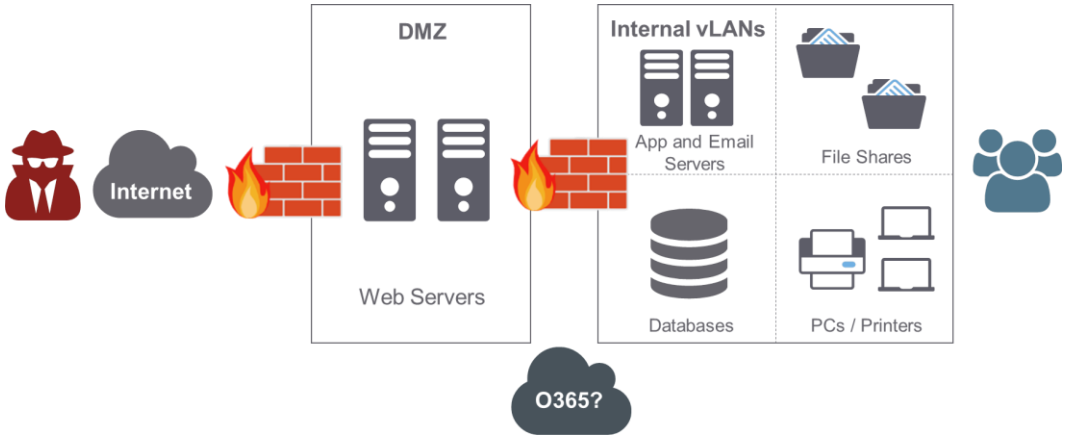
Les Very Attacked People (VAP)

proofpoint.

La stratégie defensive classique face aux tactiques des hackers

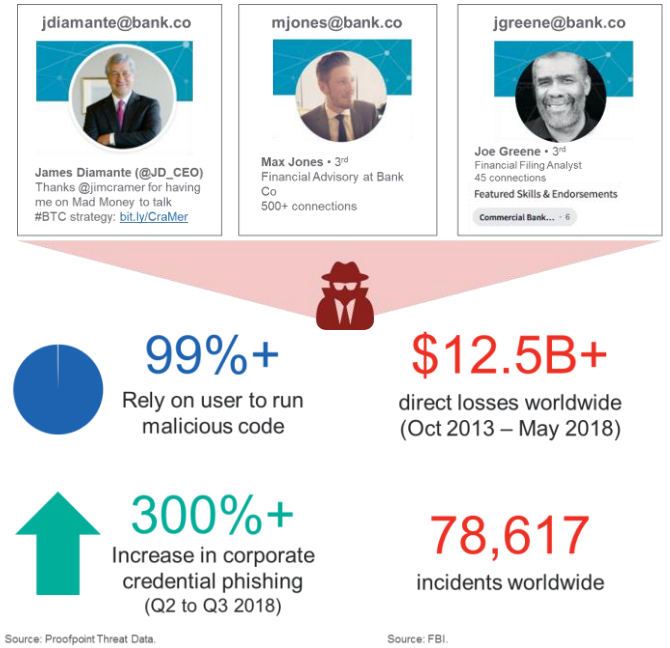
APPROCHE DEFENSIVE CLASSIQUE

Protection des ressources numériques périmétrique ou par silot

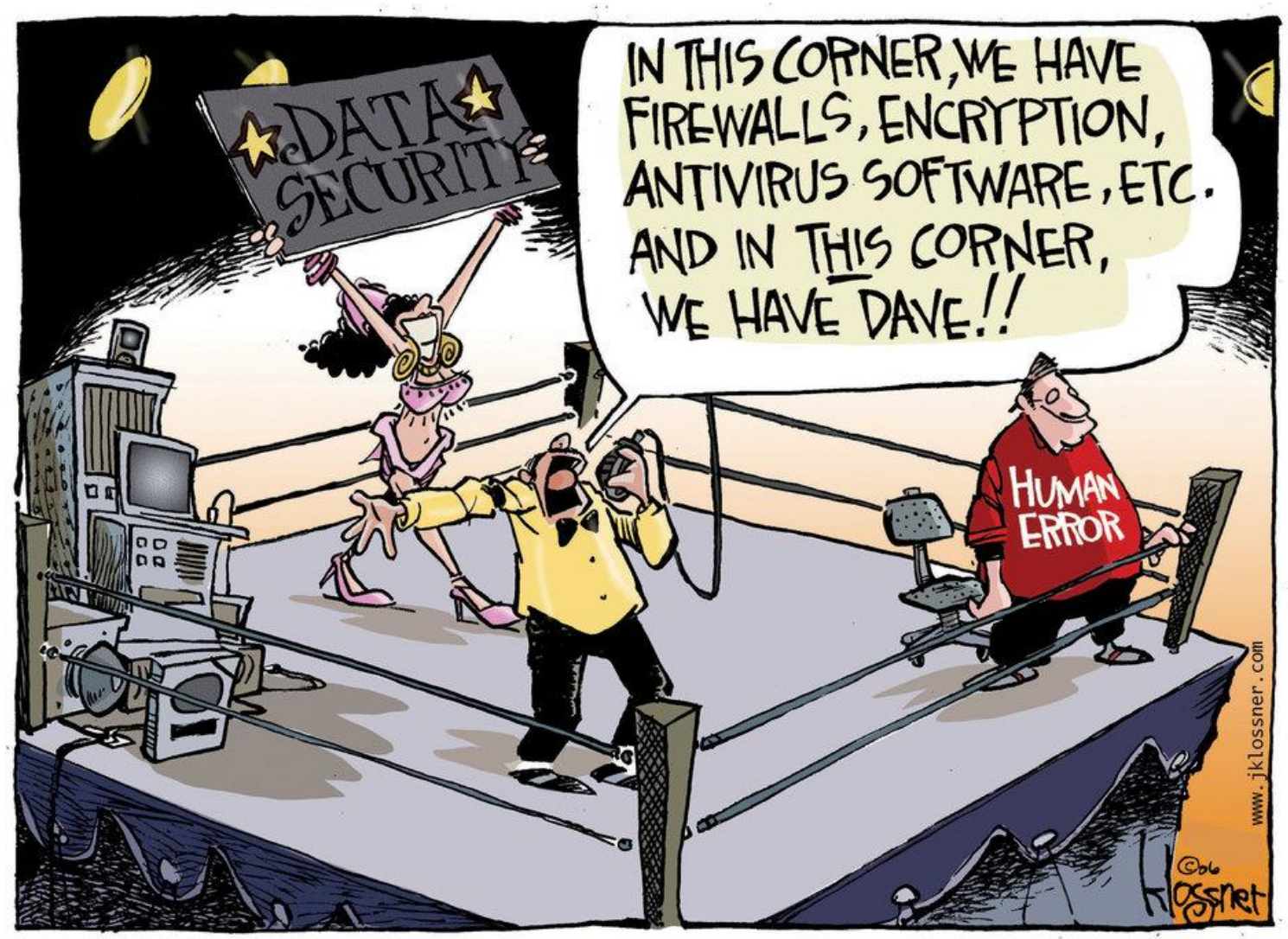


TACTIQUES d'ATTAQUES des HACKERS

Ciblage multicanal des utilisateurs



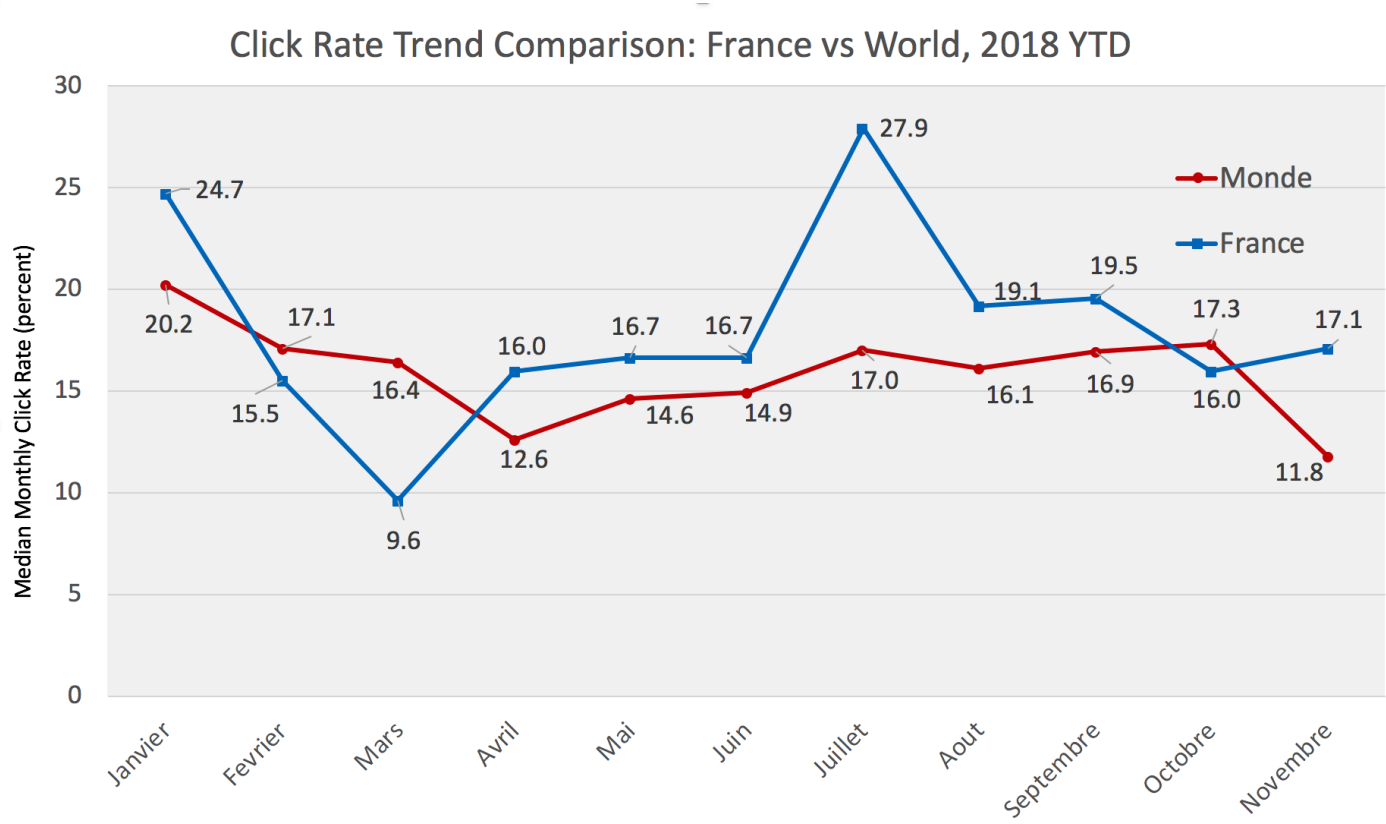
“Because Dave”



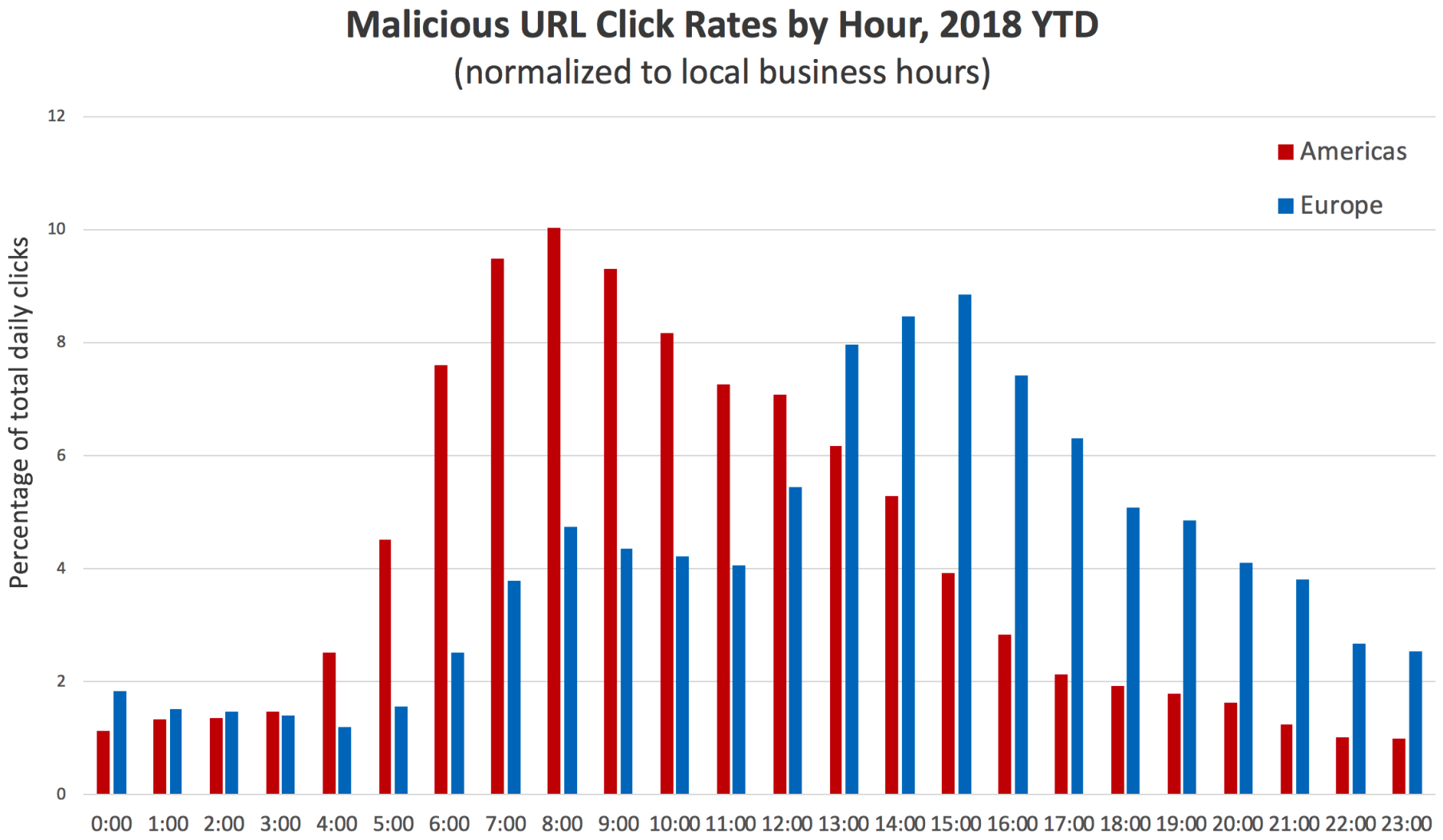
Taux de clic : France vs Global

- Taux de clic moyen :
  - France : 18%
  - Monde : 16%

- Saisonnalité du taux de clic
  - Beaucoup plus d'amplitude dans les changements
- Le taux de clic n'est pas systématiquement lié au volume de messages
- Des campagnes *TinyNuke* et *Gootkit* ciblant la France à l'été 2018 avec des templates de très bonne qualité semblent a l'origine du pic de Juillet.



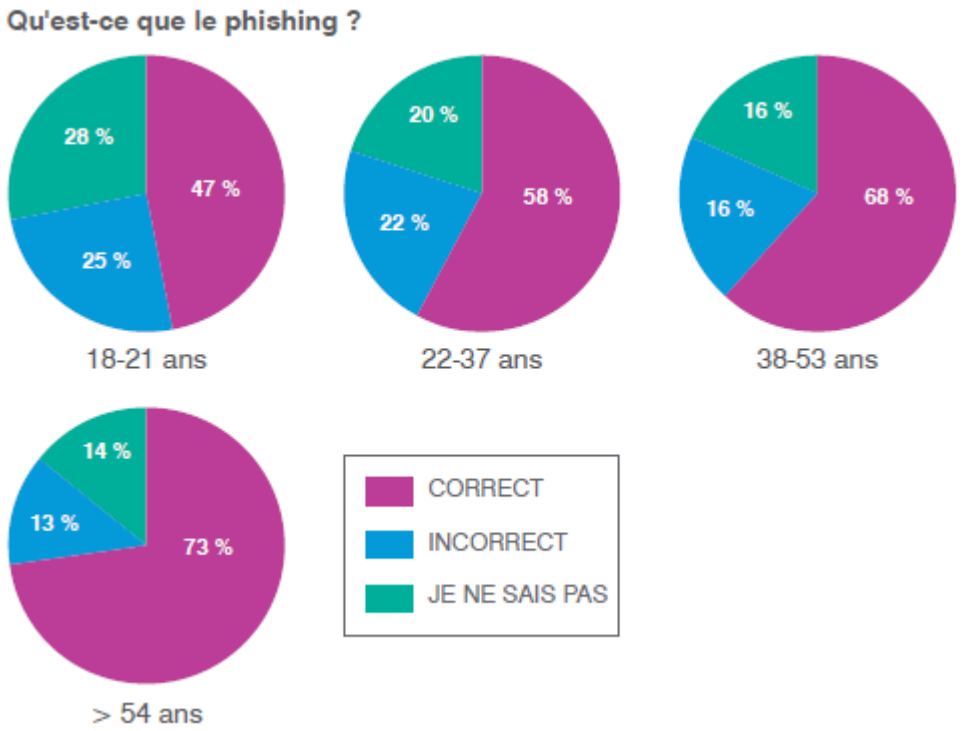
Qui clique quand ?

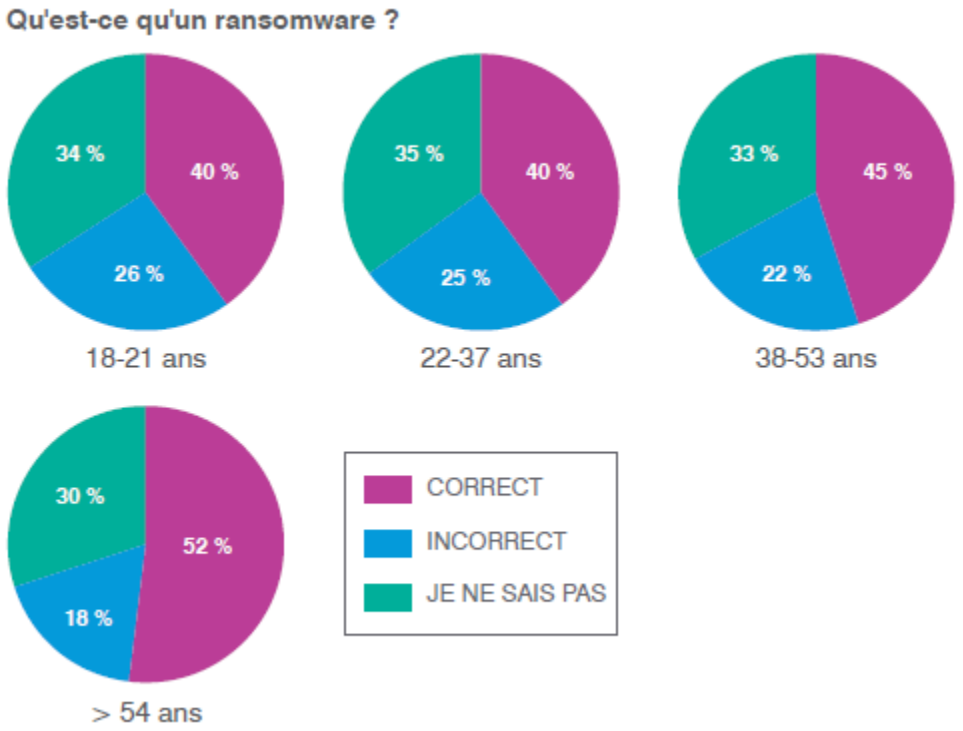


proofpoint.

Les millennials dit “digital natives” sont les moins conscients et informés des menaces !!!

(ENQUÊTE WOMBAT / REPORT OF THE PHISH 2019)

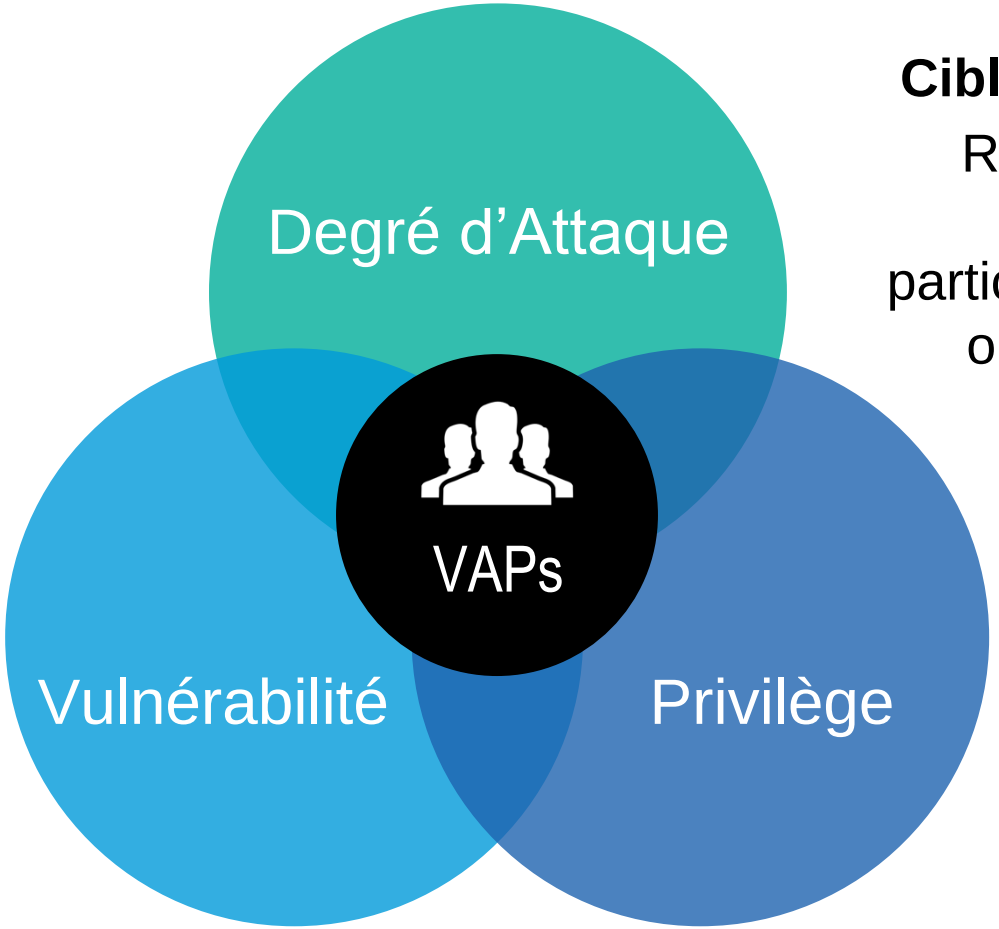




Définir les utilisateurs les plus attaqués (“Very Attacked People”)

Ciblé par les menaces

Reçoit un volume d’attaques particulièrement ciblées ou sophistiquées



Se comporte à risque au travail

Clique sur contenu malveillant, ne suit pas les campagnes de sensibilisation aux risques cyber, utilise des terminaux ou accède à des services Cloud plus risqués

Accède à des données sensibles

Accède ou gère des systèmes critiques ou des données sensibles / soumises aux conformités réglementaires (RGPD/ PII)

proofpoint.

Quantifier les VAP par un Attack Index

Sophistication de l'acteur

Degré de ciblage de l'attaque

Type d'attaque

Volume d'attaque

- Score de 0 à 1000 score par menaces envers chaque utilisateur
- Score composite pondéré

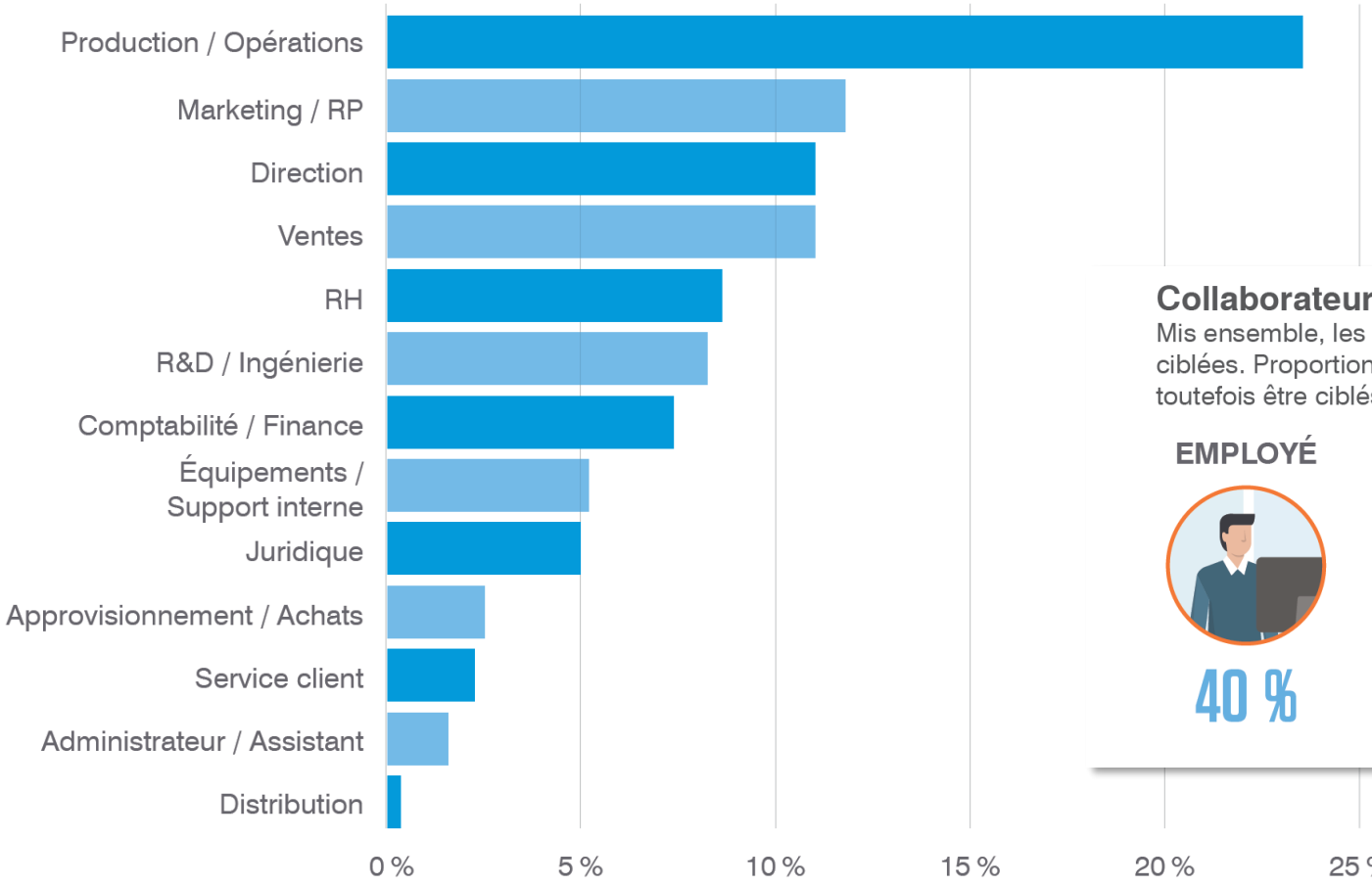
Pouvoir comprendre le risque auquel les utilisateurs font face et prioriser les mesures de sécurité qui leur sont les plus adaptées

Recevoir des rapports d'analyse précis et chiffrés de l'état des menaces qui ciblent les employés

Statistiques globales sur les Very Attacked People (VAP)

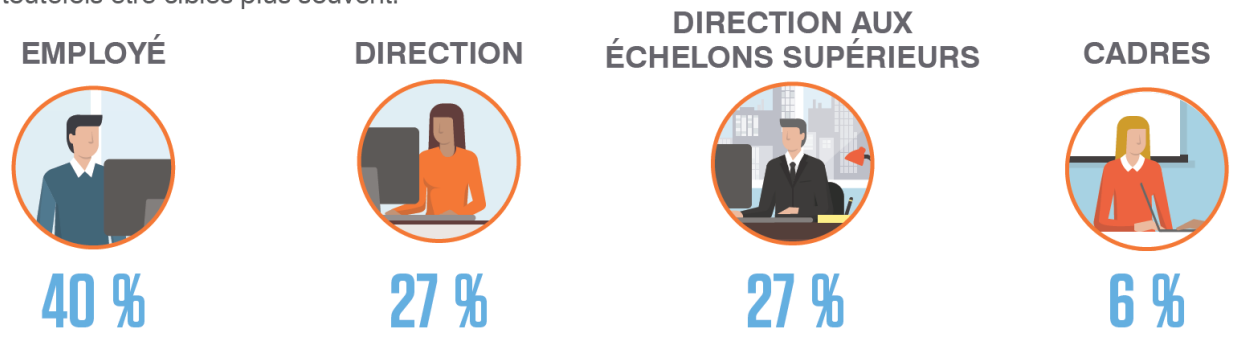
Services hautement ciblés

Les employés impliqués dans les opérations stratégiques de l'entreprise sont les plus ciblés, suivis de près par ceux des équipes d'administration et d'ingénierie.



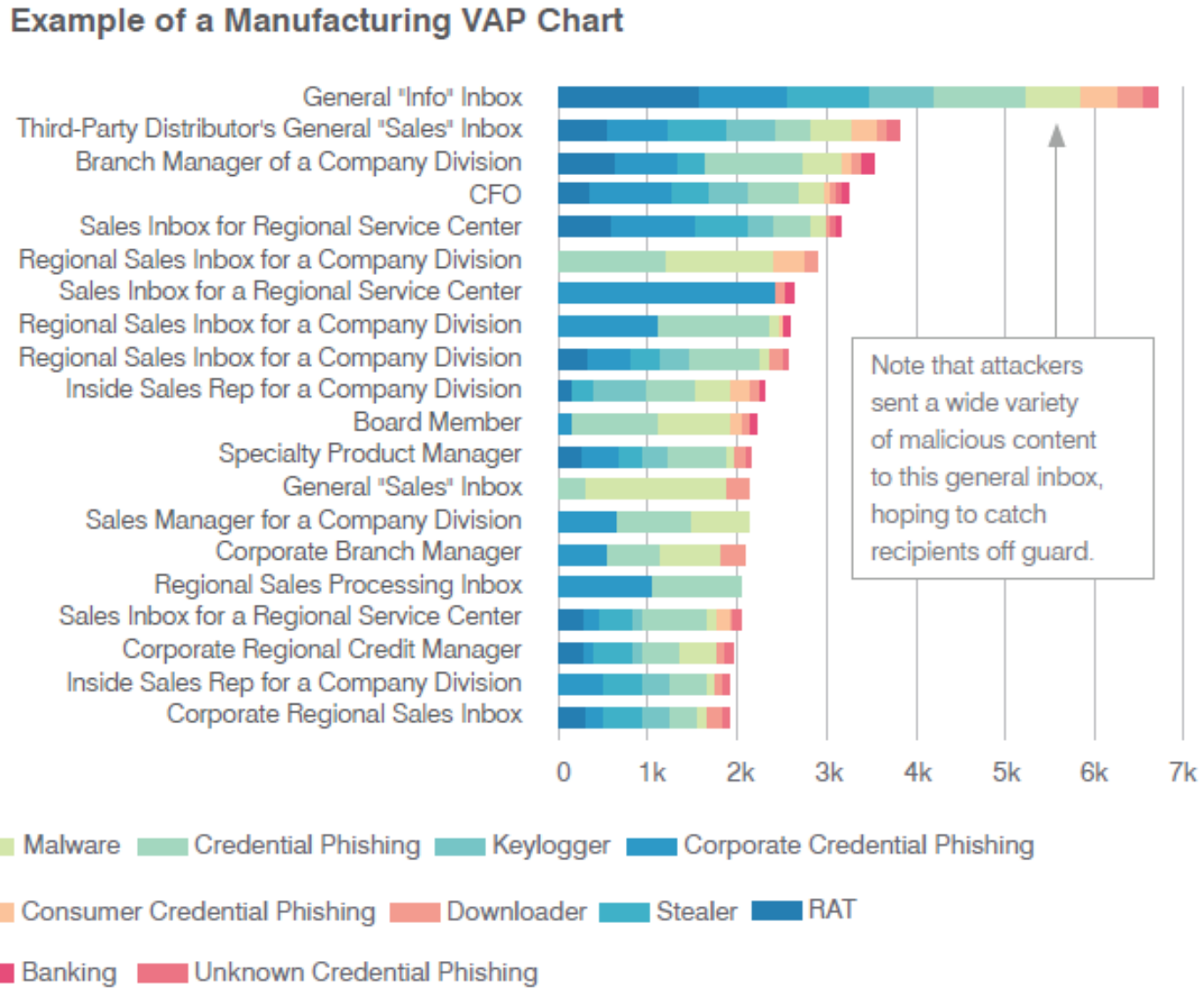
Collaborateurs hautement ciblés

Mis ensemble, les employés des échelons inférieurs sont visés par 67 % des attaques extrêmement ciblées. Proportionnellement, les cadres dirigeants, les directeurs et les chefs de service pourraient toutefois être ciblés plus souvent.



proofpoint.

Exemples de distribution d’attaques selon l’entreprise



proofpoint.

Pour approfondir

proofpoint/report-of-the-phish

proofpoint.com/human-factor