Le Facteur Humain 2025

VOL. 1 | **INGÉNIERIE SOCIALE**

proofpoint®

Introduction

L'arme la plus dangereuse d'un cyberpirate n'est pas forcément un lien malveillant ou un malware sophistiqué. Elle peut résider dans sa capacité à vous manipuler à l'aide de personnages factices, de conversations en apparence inoffensives et d'histoires plausibles. Dans les bonnes circonstances, une attaque d'ingénierie sociale astucieuse peut s'avérer aussi efficace que n'importe quelle attaque technique.

L'ingénierie sociale désigne la manipulation des émotions humaines telles que la peur, l'agacement, l'excitation ou l'urgence en vue d'inciter une victime à effectuer une action qui profite au manipulateur : passer un appel, cliquer sur un lien ou télécharger un fichier sous le contrôle insoupçonné du cybercriminel.

Les cyberattaques ciblant des personnes incluent généralement un composant d'ingénierie sociale, que ce soit un email de phishing, une fausse fenêtre contextuelle sur un site Web compromis ou même un code QR trompeur sur un autocollant. Qui plus est, il n'a jamais été aussi simple de les personnaliser. Les cybercriminels peuvent désormais cibler presque tout le monde, car l'IA générative a permis d'éliminer des obstacles tels que la langue ou l'emplacement.

Bon nombre de cybercriminels qui commettent des fraudes de type piratage de la messagerie en entreprise (BEC, Business Email Compromise), attaques par téléphone (TOAD, Telephone-Oriented Attack Delivery) et escroqueries de pig butchering ont exclusivement recours à l'ingénierie sociale. Ils évitent ainsi toute détection automatisée par des outils capables de repérer les URL et les pièces jointes malveillantes. L'objectif de ces activités est d'inciter une personne à interagir avec les cyberpirates.

Face à l'évolution constante des tactiques d'ingénierie sociale, il est naturel de se demander dans quelle mesure les utilisateurs résistent à ces attaques. Pour répondre à cette question, nous avons étudié les données de notre propre plate-forme de threat intelligence, Proofpoint Nexus®, afin de comprendre l'ampleur des défis auxquels les entreprises font face lorsqu'elles cherchent à contrer ces menaces.

Principales observations

Top 5 des thèmes d'ingénierie sociale :

1. **Fraude aux avances**
2. **Extorsion**
3. **Attaque par téléphone**
4. **Tâche rapide**
5. **Demande de devis**

25 %

25 % des campagnes APT ont exclusivement recours à l'ingénierie sociale

90 %

Plus de 90 % des campagnes APT ayant exclusivement recours à l'ingénierie sociale prétendent être intéressées par une collaboration et un engagement

50 %

La fraude aux avances a augmenté de près de 50 % au cours de l'année écoulée

70 %

Les menaces basées sur l'extorsion ont chuté de près de 70 % au cours de l'année écoulée

À propos de ce rapport

Le rapport *Le facteur humain* a toujours offert un aperçu complet des menaces centrées sur les personnes détectées, neutralisées et résolues par Proofpoint au cours des 12 mois précédents. Cette année, son format change. Plutôt que de regrouper toutes nos observations dans un seul rapport, nous allons les répartir en plusieurs volumes.

Même si chaque volume se concentrera sur une catégorie de menaces, ils partageront tous le même thème : les nouveaux développements du paysage des menaces et la façon dont la combinaison de technologie et de psychologie rend les cyberattaques modernes si dangereuses.

Portée :

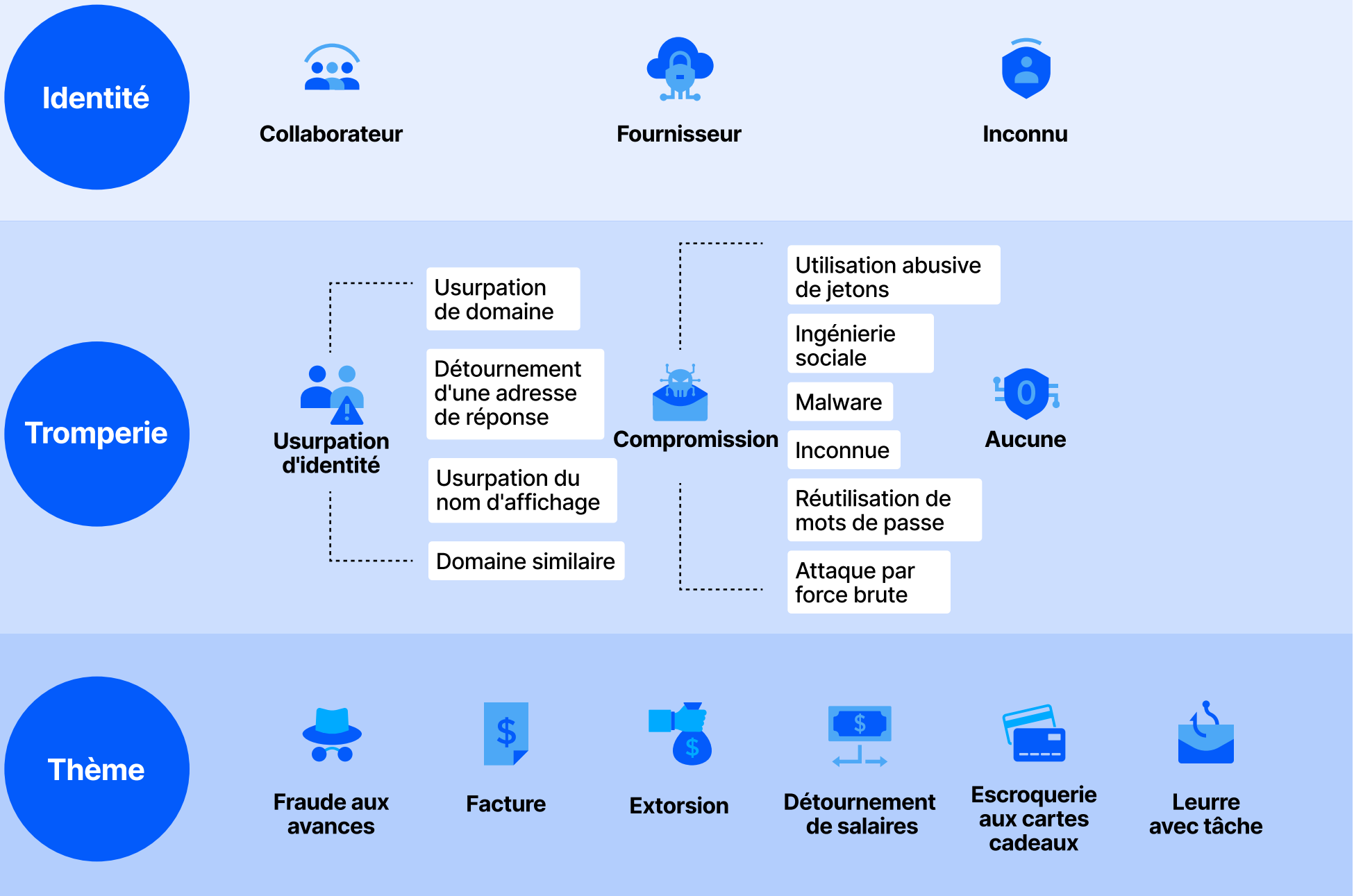
Ce rapport s'appuie sur les données collectées au sein des déploiements Proofpoint partout dans le monde, l'un des référentiels de données les plus importants et variés dans le domaine de la cybersécurité. Chaque année, nous analysons plus de **3,4 billions** d'emails, **21 billions** d'URL, **800 milliards** de pièces jointes,**1,4 billion** de SMS suspects, et bien plus encore. Les données sont issues de l'ensemble des canaux numériques pertinents.

** Couvre la période allant du 1er mars 2024 au 28 février 2025.*

Distinguer les attaques BEC des fraudes

Le terme « piratage de la messagerie en entreprise » (BEC, Business Email Compromise) est souvent employé de façon générique pour désigner une large catégorie de fraudes par email dans le cadre desquelles les cybercriminels utilisent l'ingénierie sociale pour voler des milliards de dollars par an. D'après le dernier Internet Crime Report du FBI, ces cinq dernières années, les fraudes ont coûté plus de 50 milliards de dollars aux victimes[1].

Proofpoint souhaitait mieux différencier et classer les aspects importants des fraudes par email motivées par l'appât du gain et qui ont recours à l'ingénierie sociale pour susciter une réponse de la part des cibles, au-delà des attaques BEC. C'est la raison pour laquelle nos chercheurs ont créé la taxonomie des fraudes par email.



Taxonomie des fraudes par email de Proofpoint

1. FBI, Internet Crime Report (Rapport sur la cybercriminalité), 2024.

Cette taxonomie a permis à Proofpoint de créer des détections permettant d'identifier et de différencier chaque type de fraude. Nos chercheurs s'appuient sur ces données pour mieux comprendre le paysage global, par exemple les types de thèmes d'ingénierie sociale les plus souvent utilisés par les fraudeurs — y compris les attaques BEC.

Tendances en matière de **fraude**

Proofpoint Nexus analyse plus de 2 milliards d'emails potentiellement malveillants par mois. Il s'appuie sur une analyse avancée du langage pour détecter et bloquer les attaques ayant exclusivement recours à l'ingénierie sociale à une vitesse équivalente aux attaques techniques telles que les malwares et le phishing d'identifiants de connexion.

Le jeu de règles de notre taxonomie, élaboré par des analystes humains et l'apprentissage automatique, nous permet de classer automatiquement certaines de ces activités grâce à des balises sur le thème de l'ingénierie sociale : escroqueries aux cartes cadeaux, détournement de factures et de paiements, demandes émanant de figures d'autorité (p. ex. usurpation de l'identité d'un PDG), passeurs d'argent, etc.

Après avoir filtré nos données de détection globales pour n'inclure que les types de fraudes connus associés à des balises spécifiques, nous avons pu identifier les thèmes d'ingénierie sociale les plus fréquemment observés :

Fraude aux avances

Le cybercriminel promet à la cible de lui envoyer une importante somme d'argent ou des objets de valeur en échange du paiement d'un faible montant.

Extorsion

Le cyberpirate menace la cible de lui porter physiquement atteinte ou de ternir sa réputation si elle n'accède pas à sa demande. À ne pas confondre avec les extorsions et les vols de données basés sur des ransomwares.

Attaque par téléphone (TOAD)

Le cybercriminel essaie de convaincre la cible d'appeler un numéro de téléphone, qui peut être intégré au message sous forme de texte, d'image ou de pièce jointe. Lorsque la victime appelle ce numéro, elle est invitée à installer un logiciel d'accès à distance ou à interagir avec du contenu malveillant. Chaque année, Proofpoint bloque 117 millions de menaces TOAD.

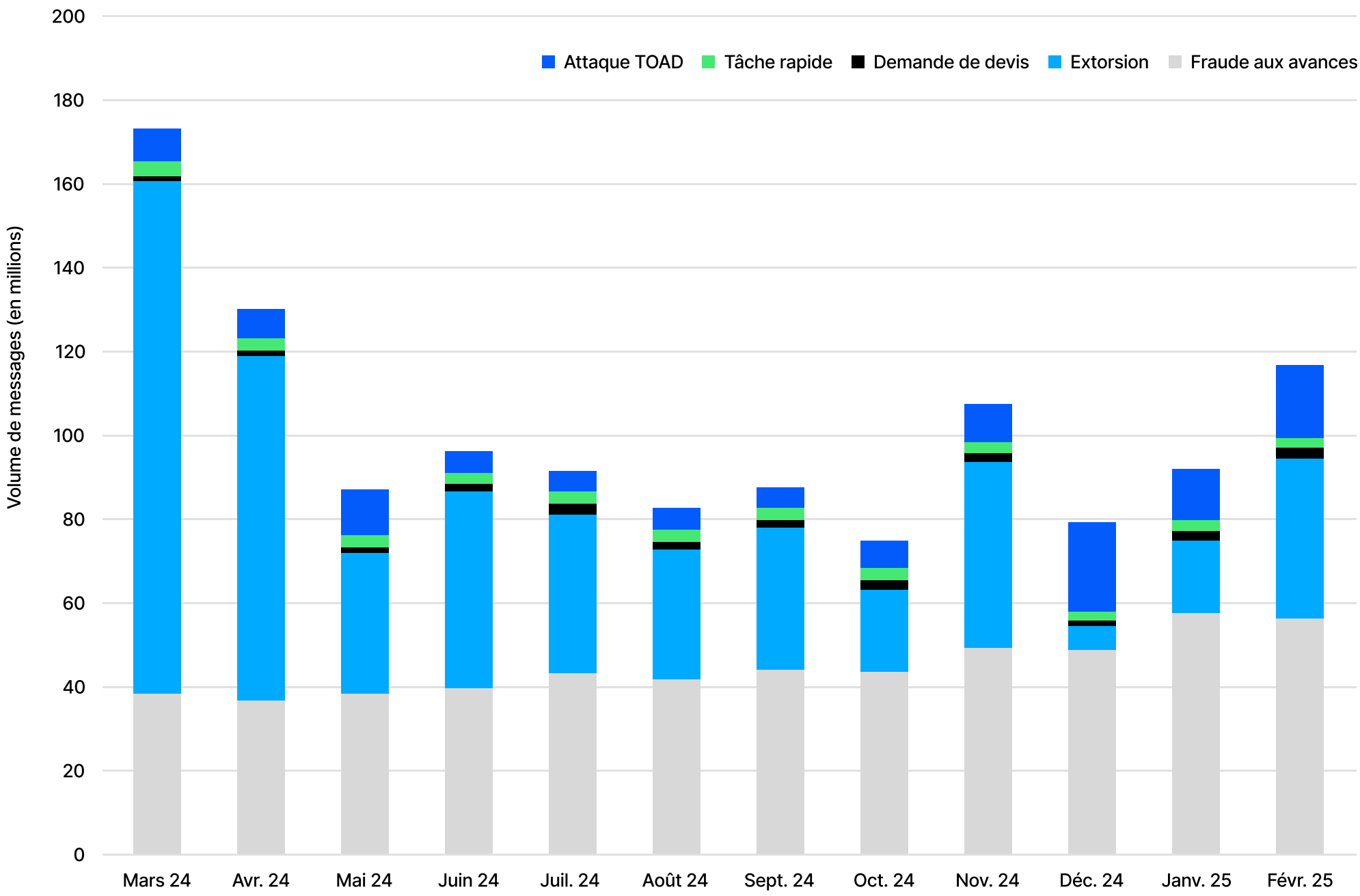
Tâche rapide

Le cyberpirate ne demande rien de spécifique, mais invite la cible à le recontacter pour effectuer une tâche précise (par exemple, un achat).

Demande de devis

Le cybercriminel envoie une fausse demande de devis, qui conduit à un vol d'argent ou à une activité secondaire telle que le déploiement d'un malware, la collecte d'identifiants de connexion ou le vol de biens physiques.

Thèmes les plus fréquemment observés dans les attaques BEC



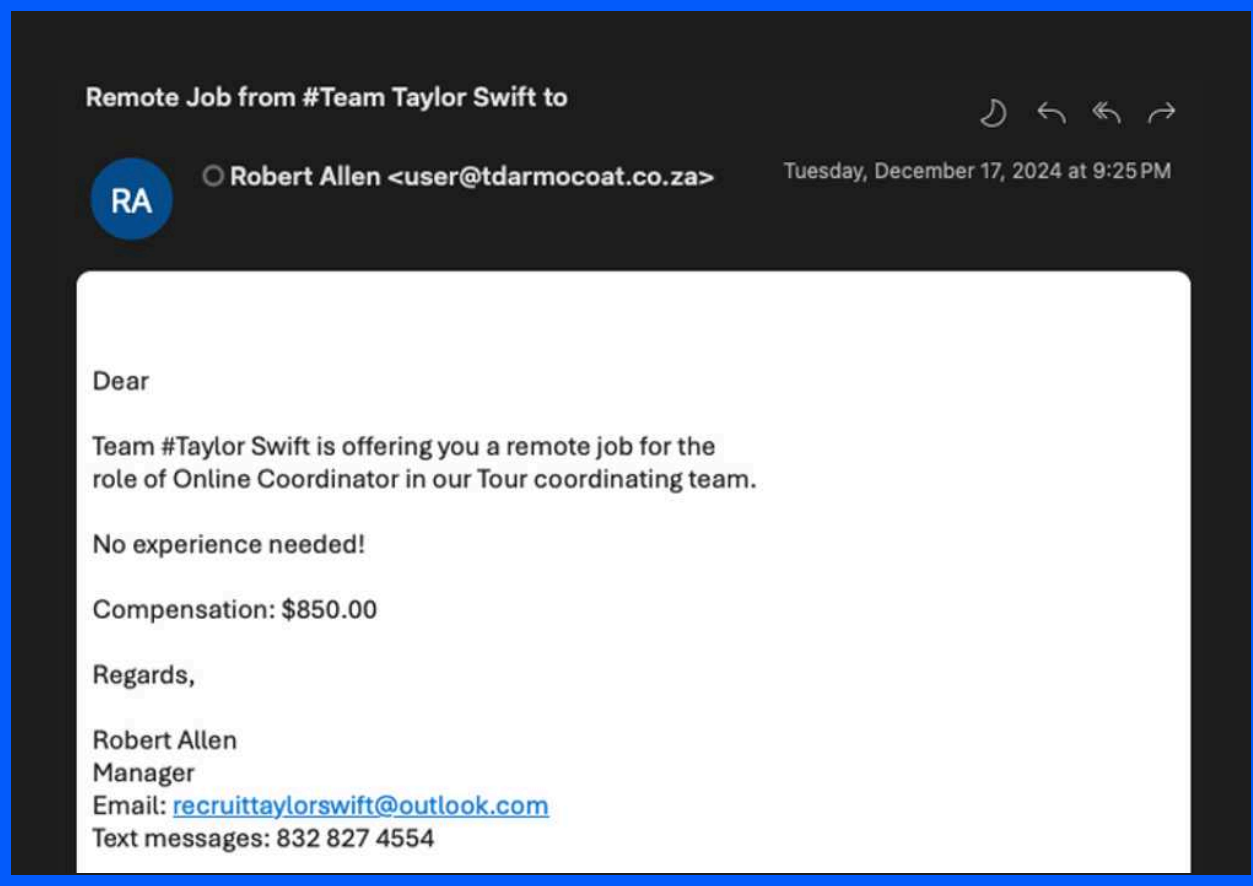
Top 5 des thèmes d'ingénierie sociale identifiés par le moteur BEC de Proofpoint Nexus

Il convient de noter que les fraudes à des fins d'extorsion diminuent dans le paysage global des menaces. Entre mars 2024 et février 2025, ces menaces ont chuté de plus de 68 %, passant de 122 millions à 38 millions par mois. Sur la même période, les fraudes aux avances ont bondi de 47 %, de 38 millions à 56 millions. Cette hausse pourrait s'expliquer par la baisse de l'efficacité des fraudes à des fins d'extorsion ou par les améliorations effectuées par les fournisseurs de services de messagerie pour contrer ces menaces spécifiques.

Ces menaces finissent toutes par voler de l'argent.

Cependant, toutes les fraudes ne se ressemblent pas. Par exemple, les cyberescrocs commettant des fraudes aux avances peuvent utiliser des emails de leurre, comme des annonces de vente de piano ou des offres d'emploi, pour inciter des victimes peu méfiantes à interagir avec eux.
En décembre 2024, de fausses offres d'emploi ont même été envoyées dans le cadre de fraudes aux avances par des cybercriminels profitant de l'engouement autour de l'Eras Tour de Taylor Swift. Les observateurs perspicaces auraient immédiatement senti le piège. Mais l'excitation engendrée par un tel email peut avoir conduit certaines personnes à tomber dans le piège.

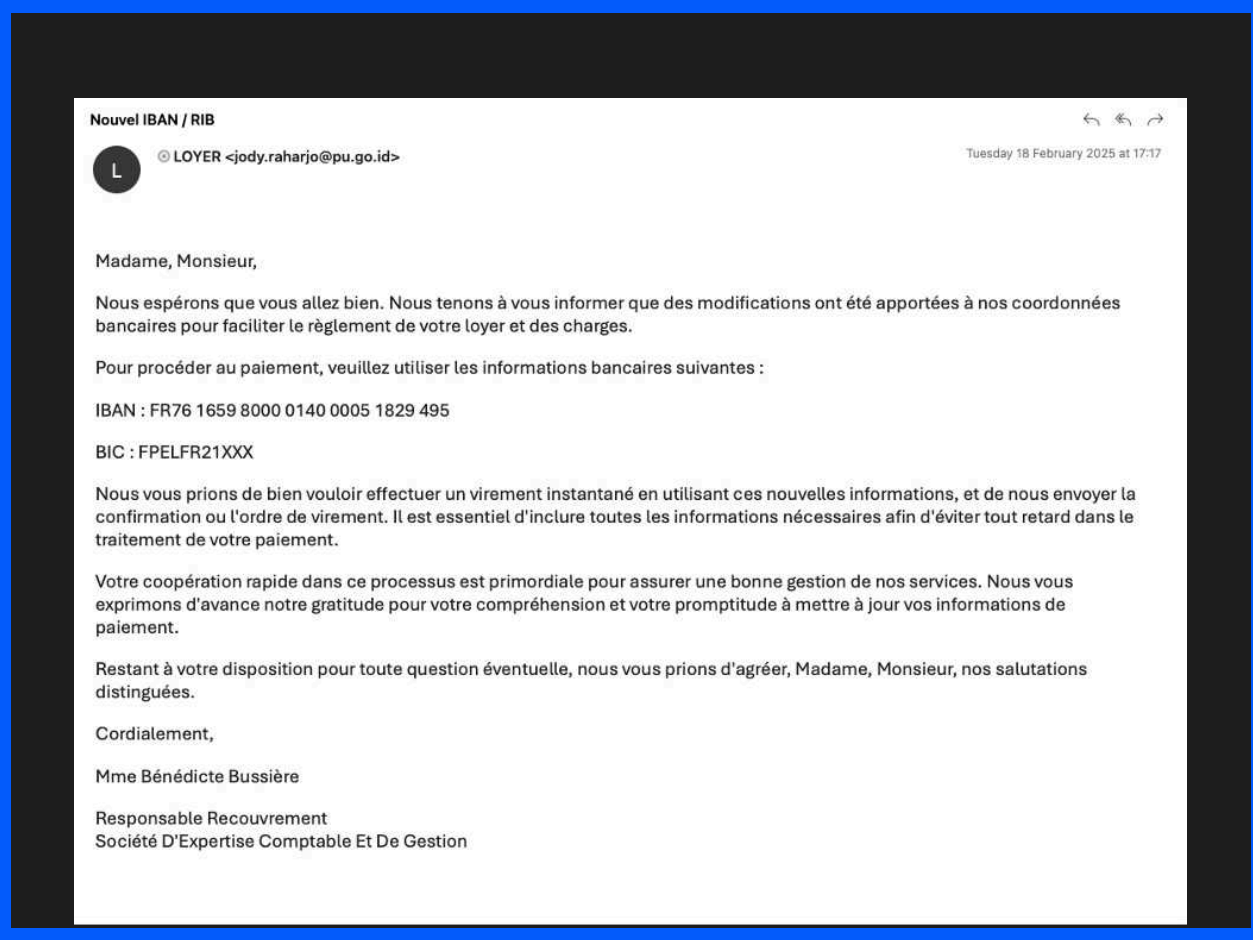
Faux email de recrutement pour l'équipe de Taylor Swift



Un problème **mondial**

Bien que la plupart des fraudes surveillées par les chercheurs soient en anglais, Proofpoint observe également des fraudes dans d'autres langues. Par exemple, un cyberescroc connu sous le nom de TA2900 envoie des emails en français concernant le paiement de loyers pour cibler des personnes en France et, occasionnellement, au Canada.

Email de phishing avec fraude au détournement de loyers



Dans ces campagnes, que Proofpoint observe plusieurs fois par semaine, les messages indiquent au destinataire que les coordonnées bancaires de l'entreprise ont changé et lui demandent d'envoyer son prochain loyer sur un nouveau compte fourni par le cybercriminel. Bien que nous ne puissions pas le confirmer, certaines formulations inhabituelles et le contenu du corps des messages laissent entendre que les emails pourraient avoir été rédigés avec l'aide de l'IA.

Avec l'essor de l'IA générative, les cyberpirates pourront probablement élargir leur réservoir de cibles en adaptant mieux l'ingénierie sociale à des emplacements et des langues spécifiques. Cependant, que les emails aient été générés avec l'IA ou par un humain, il ne faut pas oublier que la détection de ces menaces reste la même.

Des conversations **anodines**

L'ingénierie sociale consiste à amener une personne à relâcher sa vigilance. Une méthode éprouvée pour y parvenir consiste à envoyer un message anodin à une cible et à engager une conversation avec elle sur la durée. Non seulement cela permet au cybercriminel de nouer des liens avec sa cible, mais cette dernière est bien plus susceptible de lui faire confiance après une interaction soutenue en apparence crédible.

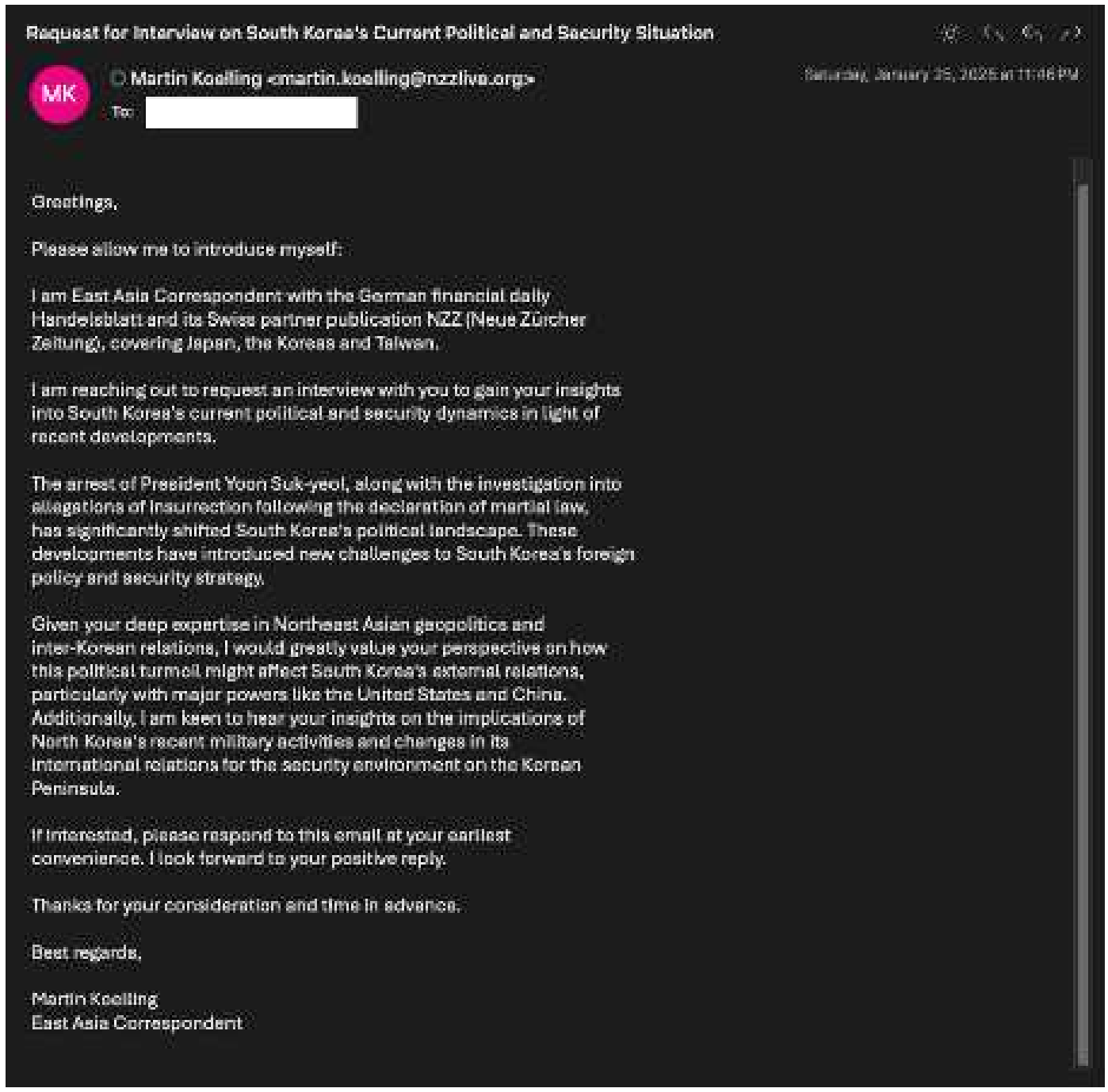
Une fois que les cyberpirates ont établi un climat de confiance, ils sont libres d'envoyer des emails contenant des URL ou des pièces jointes malveillantes, avec lesquelles la cible peut désormais être plus encline à interagir. Les cybercriminels se servent également de conversations anodines pour voir s'ils obtiennent une réponse et confirmer l'engagement. Ils évitent ainsi de griller leurs cartouches en courant le risque que leurs malwares ou une chaîne d'infection soient détectés et bloqués.

Gros plan sur les menaces APT

Alors que l'espionnage demeure la principale motivation des cybercriminels à la solde d'États, les conversations anodines font partie des outils employés par les auteurs de menaces persistantes avancées (APT) dans leurs campagnes de phishing. Ces conversations sont non seulement utilisées comme leurres pour collecter des renseignements sur la politique étrangère ou les affaires en cours, mais elles peuvent également aider les cybercriminels à obtenir des informations sur la position d'un gouvernement ou son processus de prise de décision sur une question politique. Ces informations peuvent être un atout précieux pour préparer la politique et les réactions des gouvernements qui soutiennent les cyberpirates.

Par exemple, le cybercriminel nord-coréen TA427 interagit avec des cibles pendant plusieurs semaines ou mois par le biais d'une série de conversations anodines. Il usurpe l'identité de plusieurs expéditeurs différents, mais interagit avec les cibles sur des sujets similaires, souvent liés aux affaires en cours dans la péninsule coréenne. En janvier 2025, TA427 a usurpé l'identité d'un journaliste qui cherchait à en savoir plus sur l'impact de la tentative de coup d'État et de l'arrestation ultérieure de l'ancien président sud-coréen Yoon Suk Yeol sur les politiques étrangères et de sécurité de la Corée du Sud.

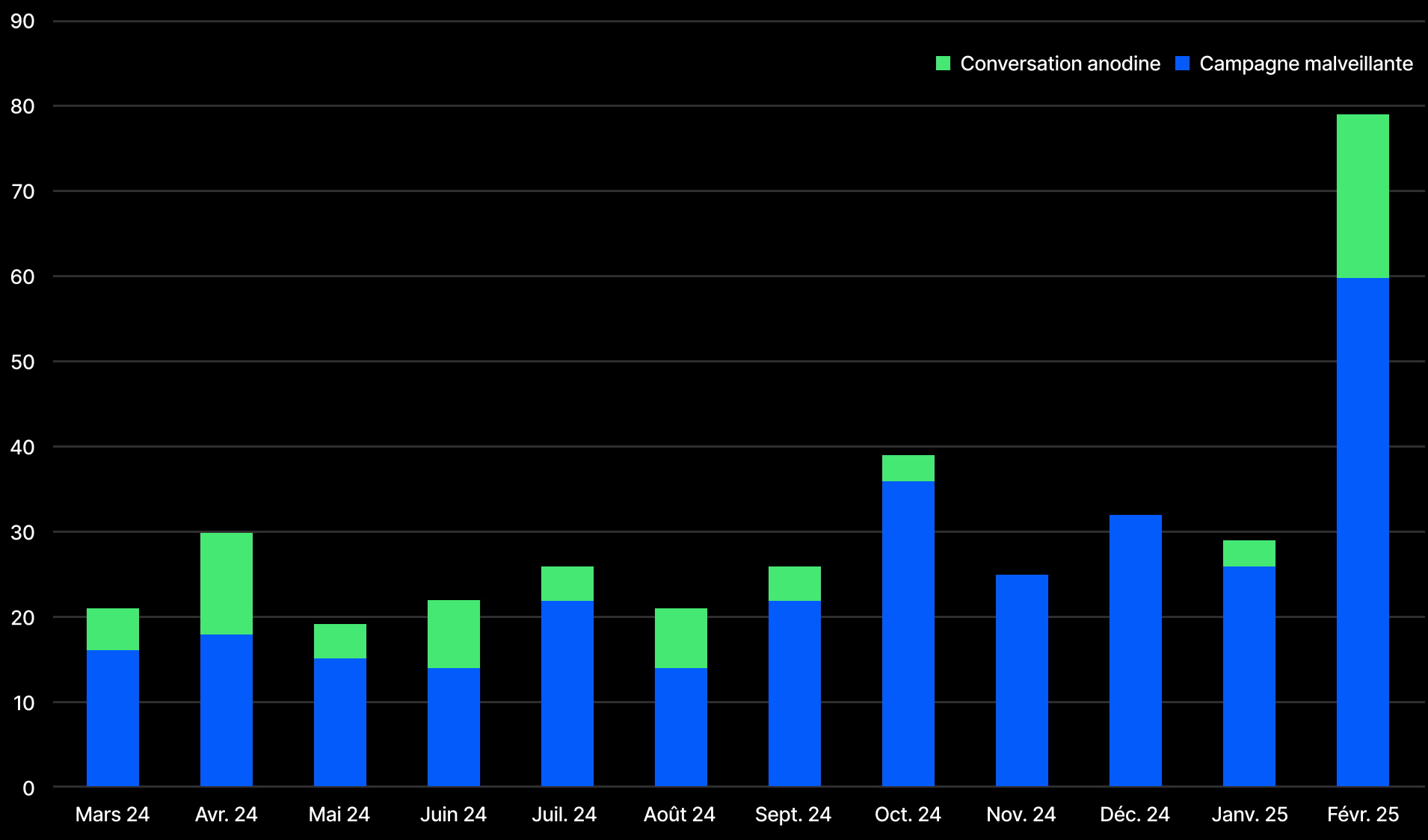
Proofpoint a également constaté que le cybercriminel iranien TA453 avait recours à des techniques similaires basées sur des conversations anodines, souvent centrées sur la situation au Moyen-Orient.



Leurre de TA427

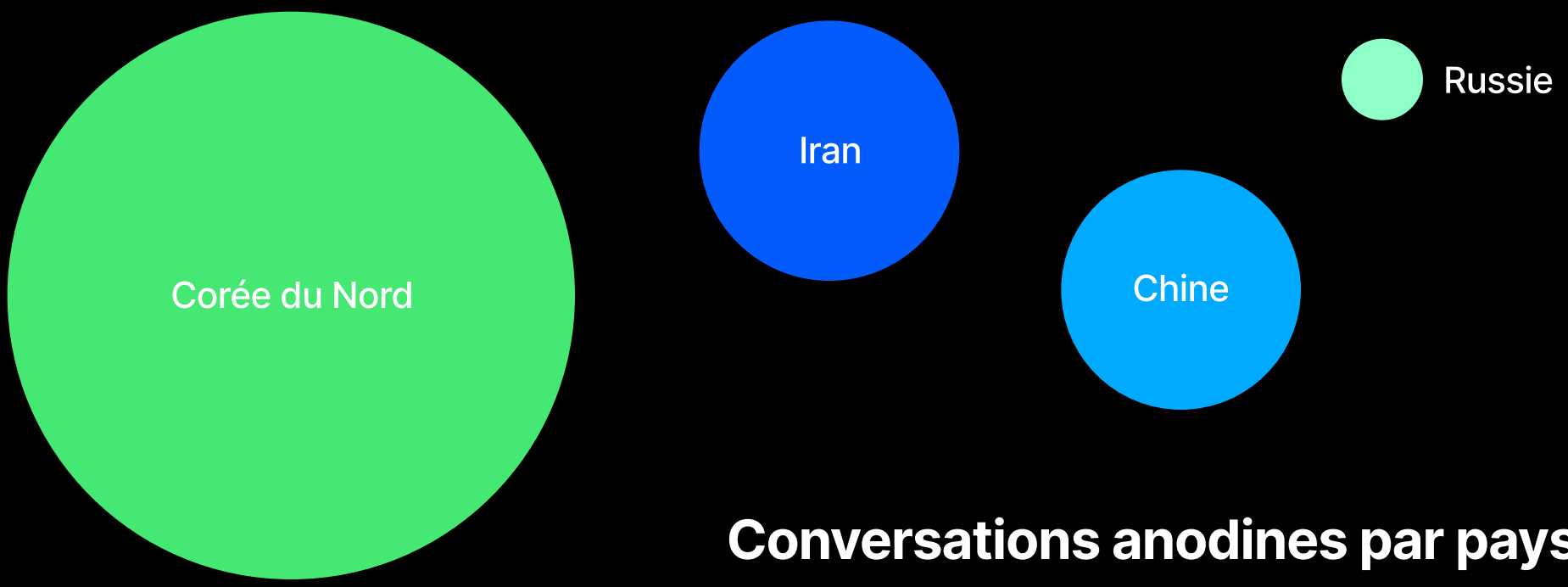
Les données issues des campagnes commanditées par des États observées au cours de l'année écoulée ont permis de mettre au jour plusieurs tendances — à la fois axées sur les données et anecdotiques. En tant que sous-ensemble des activités commanditées par des États observées, les conversations anodines représentaient environ 25 % des campagnes.

Campagnes APT observées au fil du temps



Conversations anodines et campagnes malveillantes observées sur une période d'un an

D'après les données issues des campagnes commanditées par des États observées au cours de l'année écoulée, la plupart des conversations anodines avaient été initiées par des cybercriminels nord-coréens. C'est TA427 qui a le plus utilisé de conversations anodines, comptabilisant près de 70 % des campagnes APT ayant eu recours à cette technique.



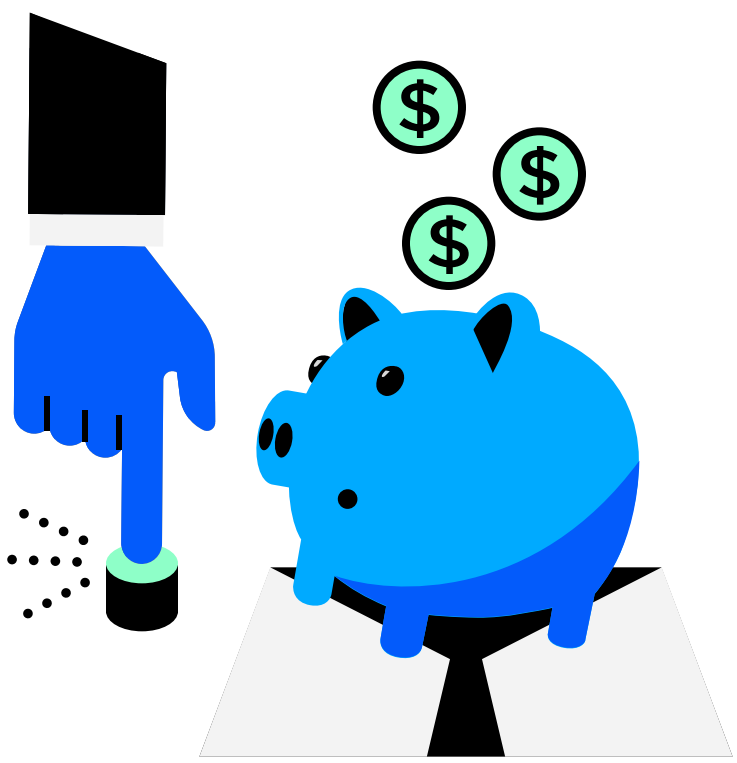
Conversations anodines par pays

Thèmes courants et tendances

Bien que les campagnes de TA427 aient fortement influencé l'ensemble de données, plusieurs tendances émergent. Sur les quelque 80 campagnes ayant eu recours à des conversations anodines documentées par les chercheurs de Proofpoint, plus de 90 % provenaient d'expéditeurs dont l'identité a été usurpée, notamment d'organisations et de personnes qui y travaillent. Il s'agissait souvent de groupes de réflexion, d'organisations gouvernementales nationales ou internationales, de médias et d'établissements universitaires.

Les expéditeurs ont préféré usurper l'identité de vraies personnes plutôt que de créer des comptes de messagerie pour de faux collaborateurs des organisations concernées, probablement dans le but de renforcer la crédibilité de leurs leurres. Dans plusieurs cas, l'adresse d'expédition usurpait le compte personnel d'une personne plutôt que son adresse email professionnelle.

Il est également intéressant de noter la constance du thème et du sujet des conversations anodines. Plus de 90 % des campagnes commanditées par des États prétendaient être intéressées par une collaboration et un engagement, qu'il s'agisse d'une invitation à participer à un événement, d'une demande de commentaire sur un sujet d'actualité ou d'une demande de rendez-vous. Toutes ces approches ont cependant un point commun : le cybercriminel tente d'obtenir une réponse en faisant l'éloge de la réputation de la cible et en sollicitant son expertise.



L'essor du pig butchering

Pendant des années, les cyberescrocs spécialisés dans le pig butchering, un type de fraude basée sur des investissements fictifs, ont utilisé des conversations anodines pour extorquer à leurs victimes des milliards de dollars en cryptomonnaie. Ces fraudeurs emploient des techniques semblables à celles des auteurs d'attaques BEC. En général, ils attirent leurs cibles dans leurs filets grâce à de longs stratagèmes d'ingénierie sociale, puis finissent par les diriger vers une fausse plate-forme d'investissement en cryptomonnaie. Selon le dernier rapport Internet Crime Report du FBI, les victimes ont fait état de plus de 6,5 milliards de dollars de pertes associées à des fraudes à l'investissement[2].

Malheureusement, ces escroqueries reposent sur des crimes réels, notamment la traite d'êtres humains. Ces derniers mois, les cyberescrocs spécialisés dans le pig butchering ont également mis en place des escroqueries plus traditionnelles telles que la fraude à l'emploi. Les revenus issus du pig butchering ont augmenté de 40 % en 2024, avec une hausse annuelle de 210 % du nombre de versements[3]. En revanche, le montant moyen des versements a diminué, les cybercriminels collectant désormais un plus grand nombre de paiements d'un montant considérablement inférieur.

2. FBI, Internet Crime Report (Rapport sur la cybercriminalité), 2024.
3. Chanalysis, « Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication » (Revenus 2024 des escroqueries aux cryptos : le pig butchering augmente de près de 40 % sur un an à mesure que les fraudes ont recours à l'IA et gagnent en sophistication), février 2025.

Conclusion

Qu'ils commettent des fraudes ou se livrent à de l'espionnage, les cybercriminels ont tous en commun une arme dans leur arsenal. Plutôt que de lancer des attaques techniquement sophistiquées, les cyberescrocs les plus futés ont recours à l'ingénierie sociale. Si les thèmes et les objectifs varient, l'objectif initial reste le même : pousser les personnes à répondre.

D'après les données de Proofpoint, dans la grande majorité des attaques, les spécificités techniques ont beaucoup moins d'importance que le facteur humain. C'est la raison pour laquelle nous recommandons d'intégrer les éléments suivants à une stratégie de défense centrée sur les personnes.

Visibilité.

Vous devez identifier les personnes ciblées et les méthodes utilisées à cette fin, ainsi que déterminer si elles sont tombées dans le piège. Il est important de connaître le risque individuel que chaque utilisateur représente : de quelle manière est-il ciblé, à quelles données a-t-il accès et a-t-il tendance à tomber dans le piège des attaques ?

Détections optimisées par l'IA.

Les menaces d'ingénierie sociale telles que les attaques TOAD et BEC ne cessent d'évoluer. Optez pour une plate-forme qui intègre une modélisation du langage en mesure de reconnaître des structures linguistiques subtiles et des indices comportementaux. Vous vous assurerez ainsi qu'elle est capable d'identifier ces menaces avant qu'elles ne puissent causer des dommages.

Protection contre l'usurpation d'identité.

Vos équipes doivent bénéficier d'une visibilité totale sur les risques tels que l'usurpation de domaines et la compromission de comptes fournisseurs. Elles doivent également disposer de contrôles pour contrer les tactiques d'usurpation d'identité, et notamment avoir la possibilité de mettre hors service et de supprimer les domaines malveillants qui imitent votre domaine.

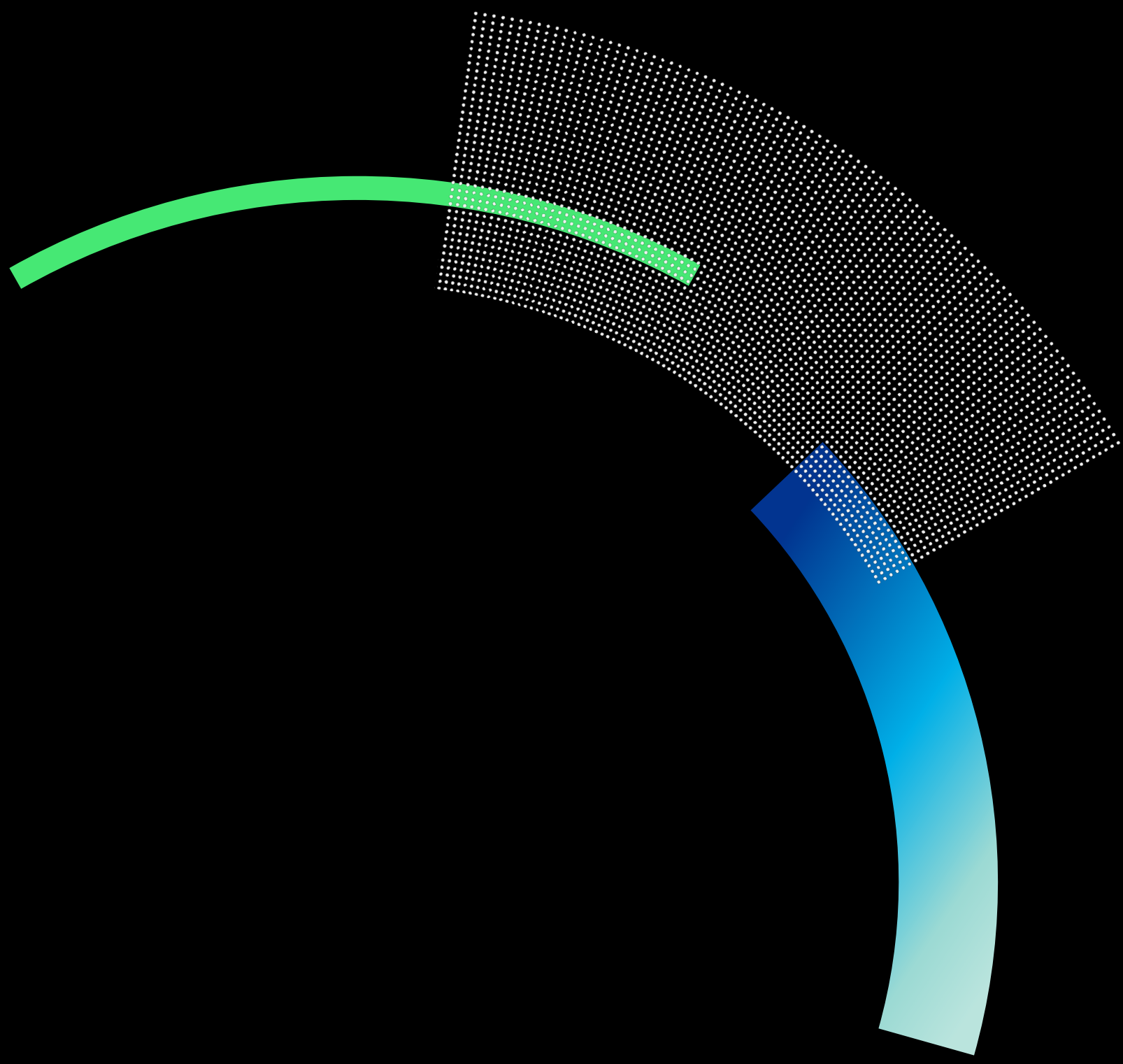
Sensibilisation personnalisée à la cybersécurité.

La formation doit être personnalisée et s'appuyer sur les informations de threat intelligence les plus récentes. Il est également essentiel de fournir aux utilisateurs des bannières d'avertissement contextuelles et des messages de formation en temps réel afin de les aider à prendre des décisions éclairées en matière de sécurité.

Workflows automatisés.

La détection, la neutralisation et la réponse aux menaces doivent être automatisées. Le volume de menaces véhiculées par email que les équipes de sécurité doivent analyser sera alors considérablement réduit.

Pour découvrir comment Proofpoint peut vous aider à évaluer les risques liés à vos utilisateurs et à les réduire, rendez-vous sur proofpoint.com/fr.



proofpoint.

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risque des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises du classement Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via la messagerie, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr.

Suivez-nous : LinkedIn

DÉCOUVRIR LA PLATEFORME PROOFPOINT →

[0400-016-03-01]