Fattore Umano 2025

VOL. 1 | **SOCIAL ENGINEERING**

proofpoint.

Introduzione

L’arma più pericolosa di un hacker non è necessariamente un link dannoso o un malware sofisticato ma potrebbe essere la sua capacità di manipolarti utilizzando personaggi fasulli, conversazioni apparentemente inoffensive e storie credibili. Nelle giuste circostanze, un attacco di social engineering ingegnoso può essere più efficace di qualsiasi attacco tecnico.

Con social engineering si intende la manipolazione delle emozioni dell’essere umano come paura, noia, eccitazione o urgenza per spingere la vittima a eseguire un’azione a vantaggio del manipolatore: effettuare una telefonata, fare clic su un link o scaricare un file sotto il controllo nascosto del criminale informatico.

Gli attacchi informatici che prendono di mira le persone solitamente includono un componente di social engineering, che sia un’email di phishing, una falsa finestra pop-up su un sito web compromesso o anche un codice QR ingannevole su un adesivo. Inoltre, sono più semplici che mai da personalizzare. Grazie all’IA generativa, i criminali informatici possono prendere di mira chiunque perché non sono più ostacolati dalla lingua o dalla posizione geografica.

Molti criminali informatici che perpetrano frodi come la violazione dell’email aziendale (BEC, Business Email Compromise), gli attacchi tramite telefonate (TOAD, Telephone-Oriented Attack Delivery) e le truffe di pig butchering utilizzano esclusivamente il social engineering. In questo modo, evitano il rilevamento automatico da parte di strumenti che possono identificare URL e allegati dannosi. L’obiettivo di queste attività è coinvolgere una persona a interagire con il criminale informatico.

Dato che i tentativi di social engineering continuano ad evolversi, è naturale chiedersi quanto gli utenti siano in grado di resistere a questi attacchi.
Per rispondere a questa domanda, abbiamo studiato i dati della nostra piattaforma di threat intelligence Proofpoint Nexus® per comprendere la portata delle sfide che le aziende devono affrontare nel cercare di gestire queste minacce.

Principali risultati

I 5 principali argomenti di social engineering:

1. **Frode con pagamento anticipato**
2. **Estorsione**
3. **Attacchi tramite telefonate**
4. **Compito veloce**
5. **Richiesta di preventivo**

25%

Il 25% di tutte le campagne APT utilizza esclusivamente il social engineering

90%

Oltre il 90% delle campagne APT che utilizzano esclusivamente il social engineering dichiara di essere interessata a una collaborazione a un coinvolgimento

50%

Le frodi con pagamento anticipato sono aumentate di quasi il 50% lo scorso anno

70%

Le minacce basate sull'estorsione sono calate di quasi il 70% lo scorso anno

Nota sul report

Fin dalla prima edizione, il report *Il fattore umano* include una panoramica completa sulle minacce incentrate sulle persone rilevate, neutralizzate e risolte da Proofpoint nei 12 mesi precedenti. Quest'anno, abbiamo cambiato il formato. Invece che riunire tutte le nostre conclusioni in un unico report, le suddividiamo in diversi volumi.

Sebbene ogni volume si concentri su una categoria di minacce, tutti condividono lo stesso argomento: i nuovi sviluppi nel panorama delle minacce e come la combinazione di tecnologia e psicologia rendono gli attacchi informatici moderni così pericolosi.

Ambito:

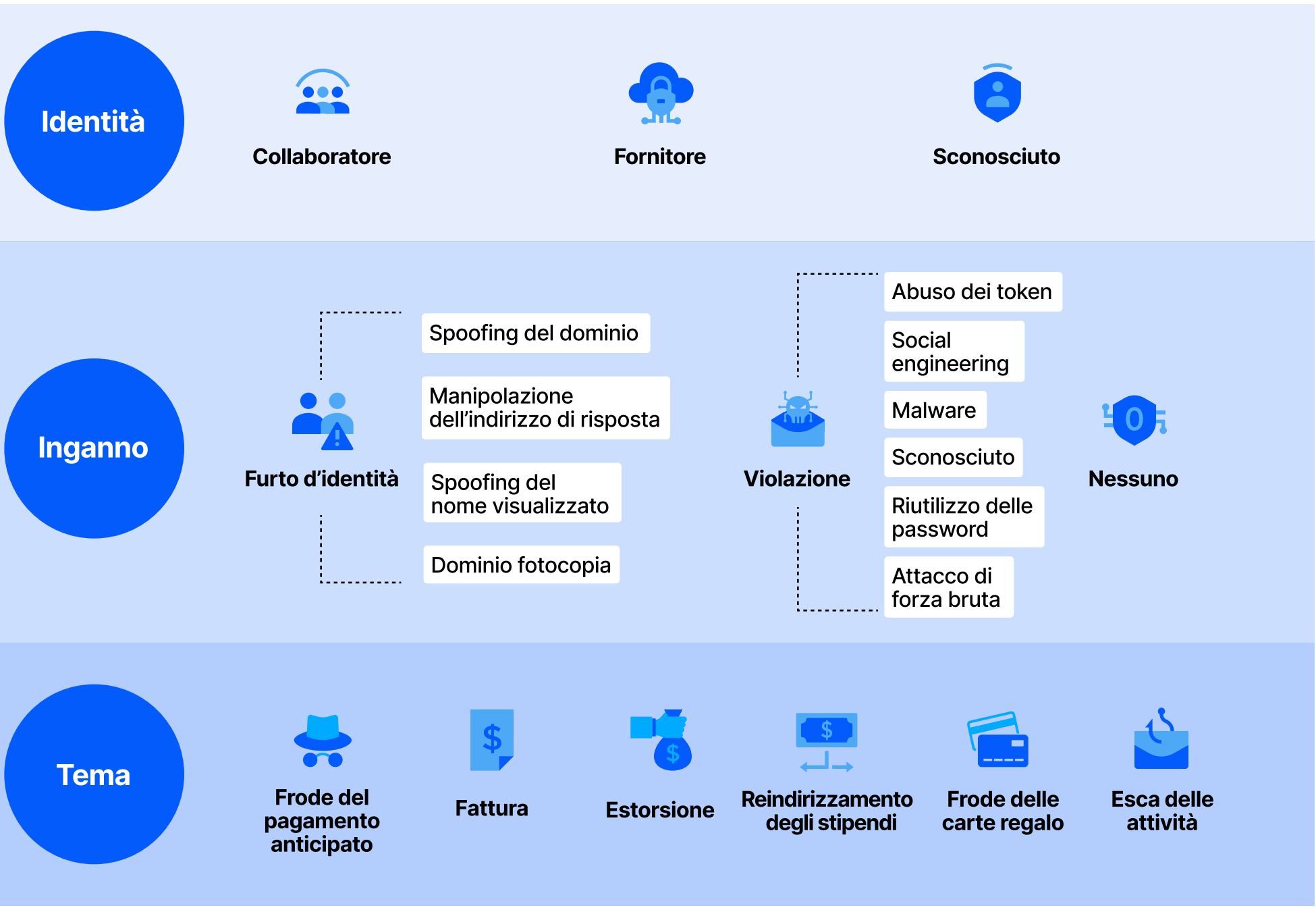
Questo report si basa sui dati raccolti dalle implementazioni di Proofpoint in tutto il mondo, una delle più grandi e diversificate serie di dati nel campo della sicurezza informatica. Ogni anno, analizziamo oltre 3,4 bilioni di messaggi email, 21 bilioni di URL, 800 miliardi di allegati, 1,4 bilioni di SMS sospetti e altro ancora.
I dati sono estratti da tutti i canali digitali rilevanti.

** Copre il periodo che va dal 1° marzo 2024 al 28 febbraio 2025.*

Distinguere gli attacchi BEC dalle frodi

Il termine "violazione dell'email aziendale" (BEC, Business Email Compromise) viene spesso utilizzato in modo generico per designare un'ampia classe di frodi via email in cui i criminali informatici utilizzano il social engineering per rubare miliardi di dollari all'anno. Secondo il più recente Internet Crime Report dell'FBI, negli ultimi cinque anni, le vittime hanno perso oltre 50 miliardi di dollari a causa di frodi[1].

Proofpoint desiderava differenziare e classificare meglio gli aspetti importanti delle frodi via email motivate dal guadagno che utilizzano il social engineering per stimolare una risposta da parte delle vittime, oltre agli attacchi BEC. Per questo motivo i nostri ricercatori hanno creato la tassonomia delle frodi via email.



1. FBI. Internet Crime Report (Report sui crimini di Internet), 2024.

Tassonomia delle frodi via email di Proofpoint

Utilizzando questa tassonomia, Proofpoint ha creato rilevamenti per identificare e differenziare ogni tipo di frode. I nostri ricercatori utilizzano questi dati per comprendere meglio il panorama complessivo, ad esempio quali tipi di argomenti di social engineering sono più utilizzati dai truffatori, inclusi gli attacchi BEC.

Tendenze delle **frodi**

Proofpoint Nexus osserva oltre 2 miliardi di email potenzialmente dannose ogni mese. La soluzione utilizza un'analisi linguistica avanzata per rilevare e bloccare gli attacchi che utilizzano esclusivamente il social engineering a una velocità equivalente agli attacchi tecnici come il malware e il phishing delle credenziali d'accesso.

L'insieme di regole della nostra tassonomia, sviluppata da analisti umani e machine learning, ci permette di classificare automaticamente alcune di queste attività grazie a tag sul tema del social engineering: frodi delle carte regalo, reindirizzamento di fatture e pagamenti, richieste da parte di figure autorevoli (come il furto d'identità del CEO), truffa dei money mule, ecc.

Dopo aver filtrato i nostri dati di rilevamento globali per includere solo i tipi di frode noti associati a tag specifici, questi sono gli argomenti di social engineering osservati che abbiamo osservato più di frequente:

Frode del pagamento anticipato

Il criminale informatico promette all'obiettivo una somma di denaro significativa o articoli di valore elevato in cambio di un piccolo pagamento.

Estorsione

Il criminale informatico minaccia l'obiettivo di danni fisici o danneggiamento della sua reputazione se non dà seguito alla sua richiesta. È una minaccia diversa dai furti e dalle estorsioni di dati basati sul ransomware.

Attacchi tramite telefonate (TOAD)

Il criminale informatico cerca di convincere l'obiettivo a chiamare un numero di telefono, che potrebbe essere incluso nel messaggio come testo, immagine o allegato. Quando la vittima chiama questo numero, viene convinta a installare un software di accesso remoto o comunque interagire con contenuti dannosi. Proofpoint blocca 117 milioni di minacce TOAD ogni anno.

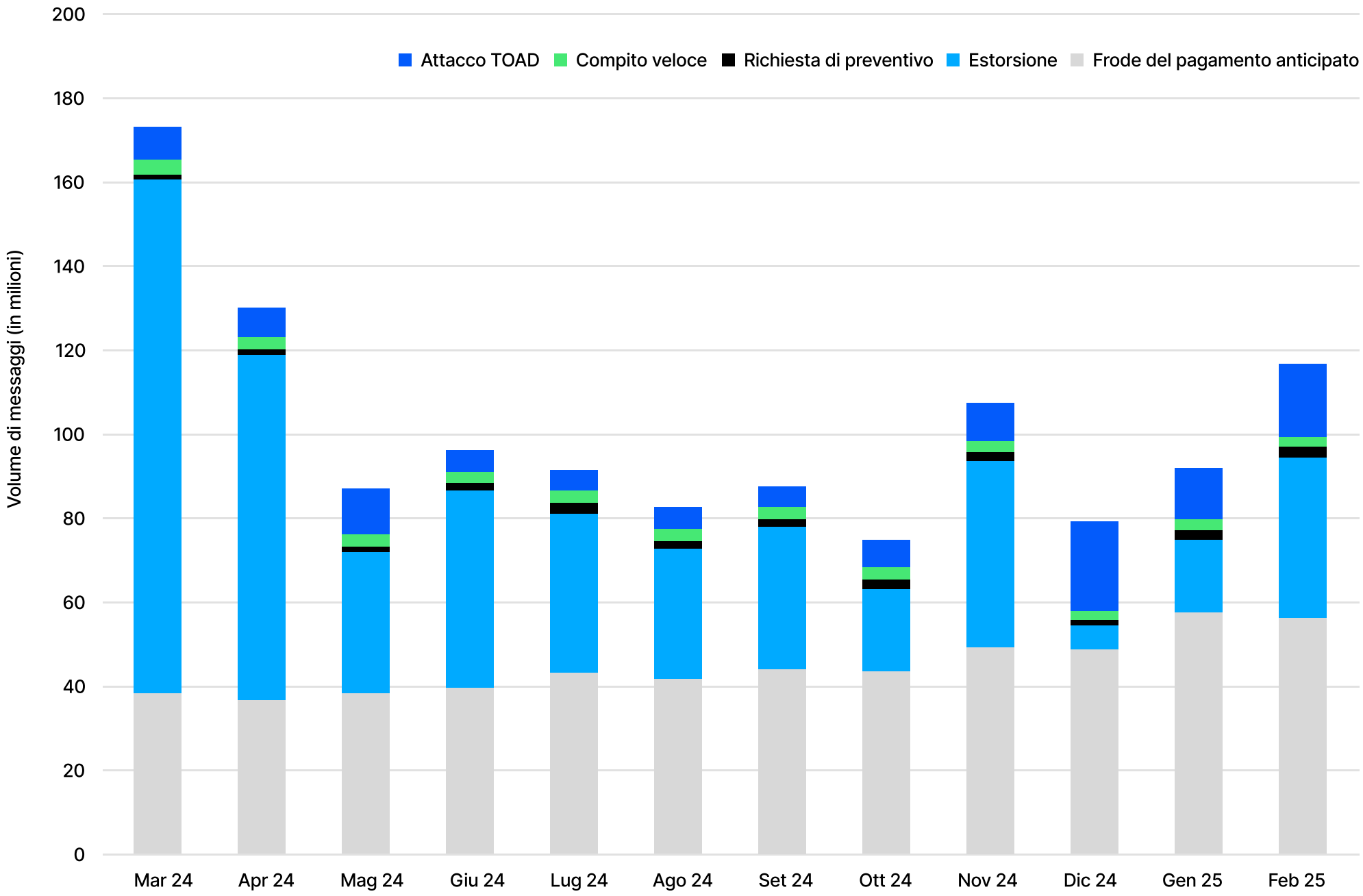
Compito veloce

Il criminale informatico non richiede niente di specifico, ma invita l'obiettivo a ricontattarlo per portare a termine un determinato compito, come effettuare un acquisto.

Richiesta di preventivo

Il criminale informatico invia una richiesta fasulla per un preventivo, che porta a un furto di denaro o attività successive come la distribuzione di malware, raccolta delle credenziali di accesso o furto di beni fisici.

Argomenti osservati più di frequente negli attacchi BEC

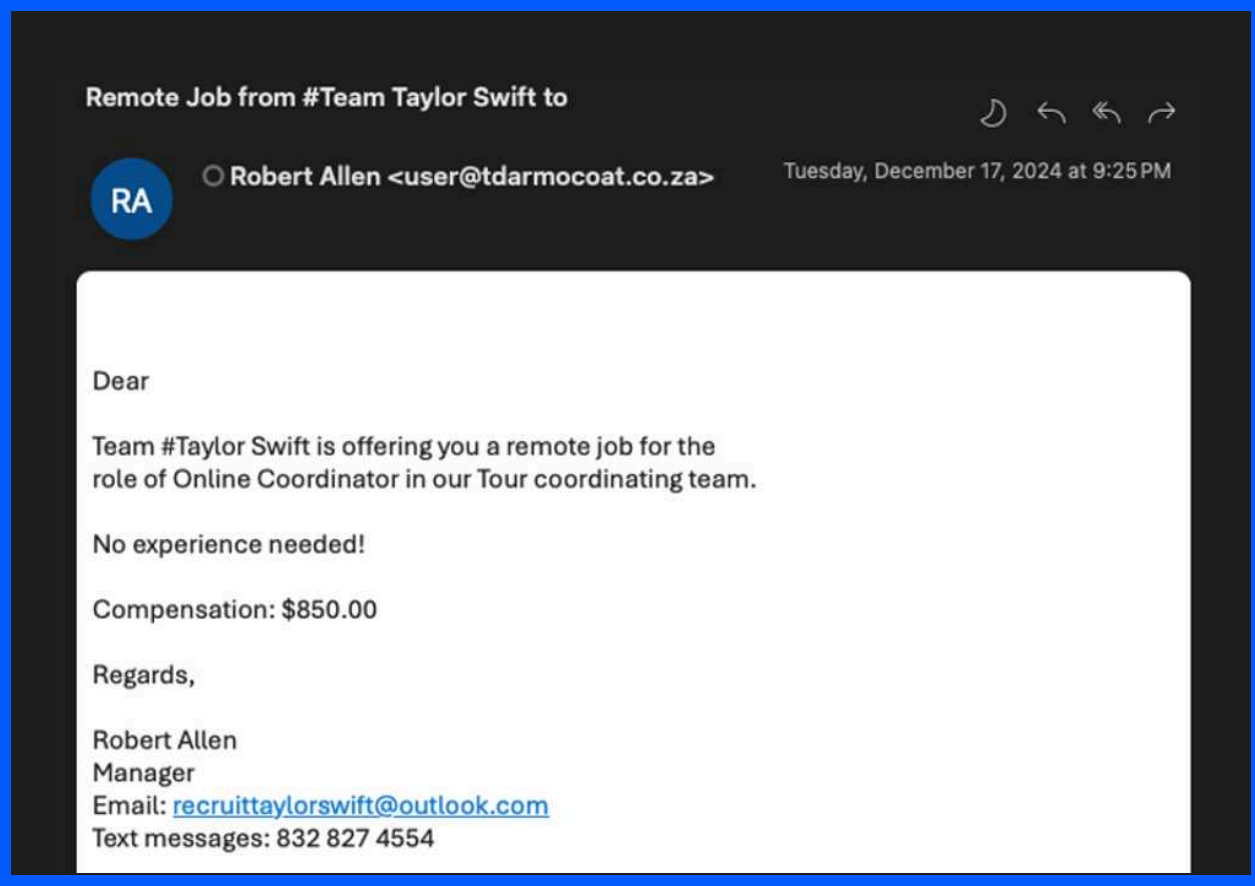


I primi 5 argomenti di social engineering identificati dal motore BEC di Proofpoint Nexus

In particolare, le frodi a fini di estorsione sono in calo nel panorama complessivo delle minacce. Tra marzo 2024 e febbraio 2025, queste minacce sono scese di oltre il 68%, passando da 122 milioni a 38 milioni al mese. Nello stesso intervallo temporale, le minacce delle frodi con pagamento anticipato sono aumentate del 47% da 38 milioni a 56 milioni. Questo aumento potrebbe essere dovuto alla minor efficacia delle frodi a fini di estorsione oppure per i miglioramenti apportati dai fornitori di servizi email per contrastare queste minacce specifiche.

Queste minacce finiscono tutte per rubare denaro.

Tuttavia non tutte le frodi sono uguali. Per esempio, i truffatori che perpetrano frodi con pagamento anticipato possono utilizzare email ingannevoli come annunci di pianoforte in vendita o offerte di lavoro per attirare vittime ignare a interagire con loro. Nel dicembre 2024, false offerte di lavoro sono state inviate nell’ambito delle frodi con pagamento anticipato da criminali informatici che hanno approfittato del clamore intorno all’Eras Tour di Taylor Swift. Gli osservatori più accorti avrebbero subito capito che si trattava di una truffa. Ma l'eccitazione provocata da un'email del genere potrebbe aver spinto alcune persone a farsi ingannare.


Remote Job from #Team Taylor Swift to

RA

Robert Allen <user@tdarmocoat.co.za>

Tuesday, December 17, 2024 at 9:25 PM

Dear

Team #Taylor Swift is offering you a remote job for the role of Online Coordinator in our Tour coordinating team.

No experience needed!

Compensation: $850.00

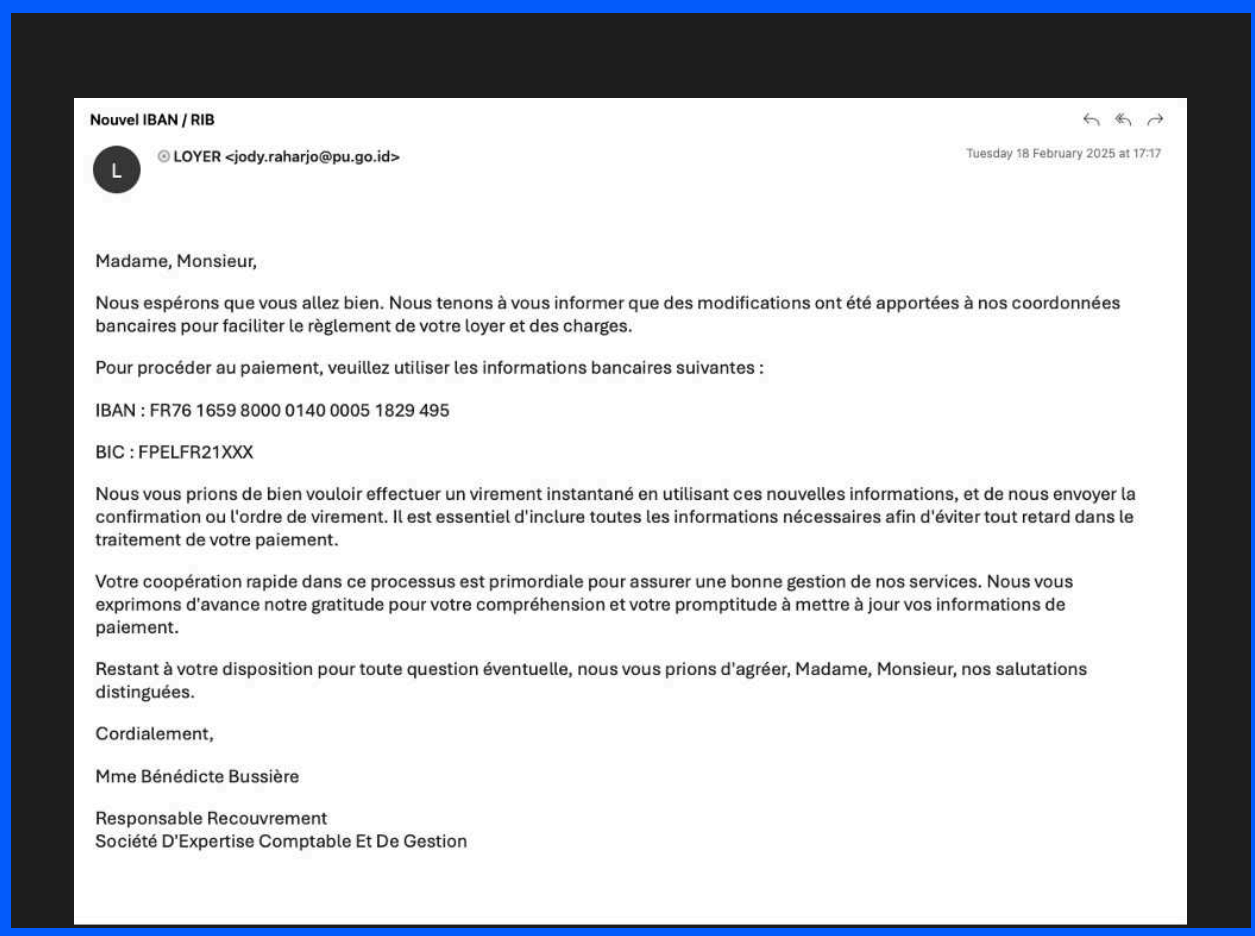
Regards,

Robert Allen
Manager
Email: recruittaylorswift@outlook.com
Text messages: 832 827 4554

Email fasulla di offerta di lavoro dal team di Taylor Swift.

Un problema **globale**

Anche se la maggior parte delle frodi monitorate dai ricercatori è in inglese, Proofpoint ha osservato anche frodi in altre lingue. Per esempio, un truffatore noto come TA2900 invia email in lingua francese utilizzando argomenti sul pagamento di affitti per colpire persone in Francia e, occasionalmente, in Canada.


Nouvel IBAN / RIB

L

LOYER <jody.raharjo@pu.go.id>

Tuesday 18 February 2025 at 17:17

Madame, Monsieur,

Nous espérons que vous allez bien. Nous tenons à vous informer que des modifications ont été apportées à nos coordonnées bancaires pour faciliter le règlement de votre loyer et des charges.

Pour procéder au paiement, veuillez utiliser les informations bancaires suivantes :

IBAN : FR76 1659 8000 0140 0005 1829 495

BIC : FPELFR21XXX

Nous vous prions de bien vouloir effectuer un virement instantané en utilisant ces nouvelles informations, et de nous envoyer la confirmation ou l'ordre de virement. Il est essentiel d'inclure toutes les informations nécessaires afin d'éviter tout retard dans le traitement de votre paiement.

Votre coopération rapide dans ce processus est primordiale pour assurer une bonne gestion de nos services. Nous vous exprimons d'avance notre gratitude pour votre compréhension et votre promptitude à mettre à jour vos informations de paiement.

Restant à votre disposition pour toute question éventuelle, nous vous prions d'agréer, Madame, Monsieur, nos salutations distinguées.

Cordialement,

Mme Bénédicte Bussière

Responsable Recouvrement
Société D'Expertise Comptable Et De Gestion

Email di phishing con appropriazione fraudolenta degli affitti.

In queste campagne, che Proofpoint osserva più volte alla settimana, i messaggi informano il destinatario che le coordinate bancarie dell'azienda sono cambiate e gli richiede di inviare il suo prossimo pagamento a un nuovo conto fornito dal criminale informatico. Pur non potendo confermarlo, alcune frasi insolite e il contenuto del corpo delle email, lasciano intendere che le email potrebbero essere state scritte con l'aiuto dell'intelligenza artificiale.

L'IA generativa è sempre più comune e i criminali informatici saranno probabilmente in grado di ampliare il loro bacino di utenza adattando meglio il social engineering a luoghi e lingue specifiche. Ma è importante ricordare che non ha importanza se le email sono state generate da un essere umano o attraverso l'IA, il rilevamento di queste minacce rimane lo stesso.

Conversazioni **innocue**

Il social engineering consiste nel far abbassare la guardia a una persona. Un metodo comprovato per raggiungere questo scopo consiste nell'inviare un messaggio innocuo a un obiettivo e inviare una conversazione nel tempo. Ciò contribuisce non solo a creare una relazione con l'obiettivo, ma quest'ultimo sarà più propenso a fidarsi del criminale informatico dopo un'interazione continua in apparenza credibile.

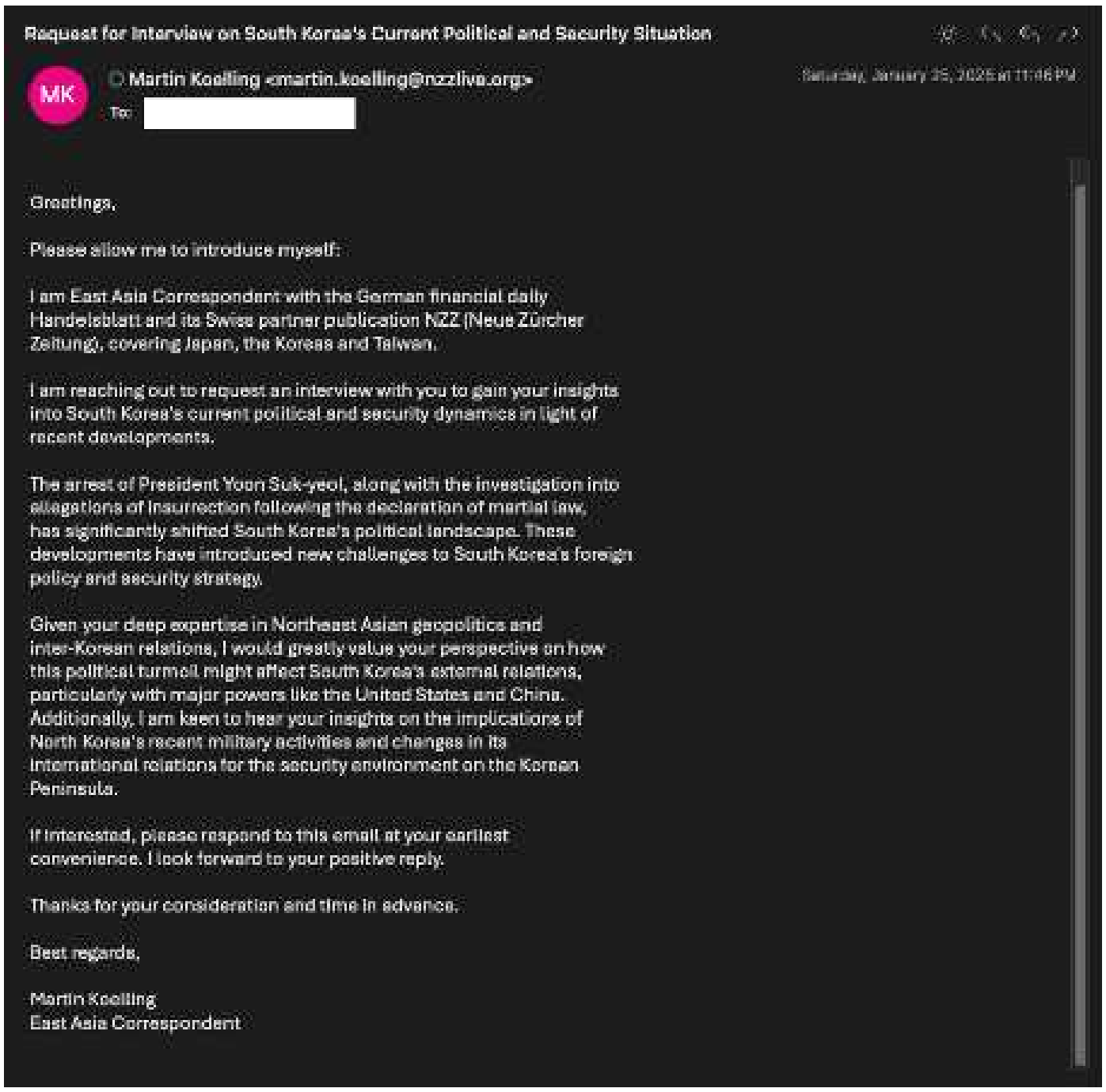
Una volta che i criminali informatici hanno instaurato un rapporto di fiducia, possono inviare email che contengono link o allegati dannosi, con i quali l'obiettivo potrebbe essere più propenso a interagire. I criminali informatici utilizzano conversazioni innocue anche per vedere se ottengono una risposta e confermare il coinvolgimento. Ciò li aiuta a evitare il rischio che il loro malware o una catena di infezione siano rilevati e bloccati.

Minacce APT in evidenza

Lo spionaggio continua a essere la principale motivazione per i criminali al soldo degli Stati e le conversazioni innocue sono uno strumento che i gruppi criminali delle minacce persistenti avanzate (APT) utilizzano nelle loro campagne di phishing. Queste conversazioni non solo vengono utilizzate come esche per acquisire informazioni sulla politica estera o le attività in corso, ma possono anche aiutare i criminali informatici a ottenere informazioni sulla posizione di un governo o il processo decisionale su una problematica politica. Queste informazioni possono essere un contributo prezioso alla definizione delle politiche e delle reazioni dei governi che sponsorizzano i criminali informatici.

Per esempio, il criminale informatico nordcoreano TA427 interagisce con gli obiettivi per settimane o mesi utilizzando una serie di conversazioni innocue. Ruba l'identità di numerosi mittenti diversi, ma interagisce con gli obiettivi su oggetti simili, spesso legati agli affari in corso nella penisola coreana. Nel gennaio 2025, TA427 ha rubato l'identità di un giornalista che cercava di saperne di più sull'impatto del tentato colpo di Stato e del successivo arresto dell'ex presidente sudcoreano Yoon Suk Yeol sulla politica estera e relativa alla sicurezza della Corea del Sud.

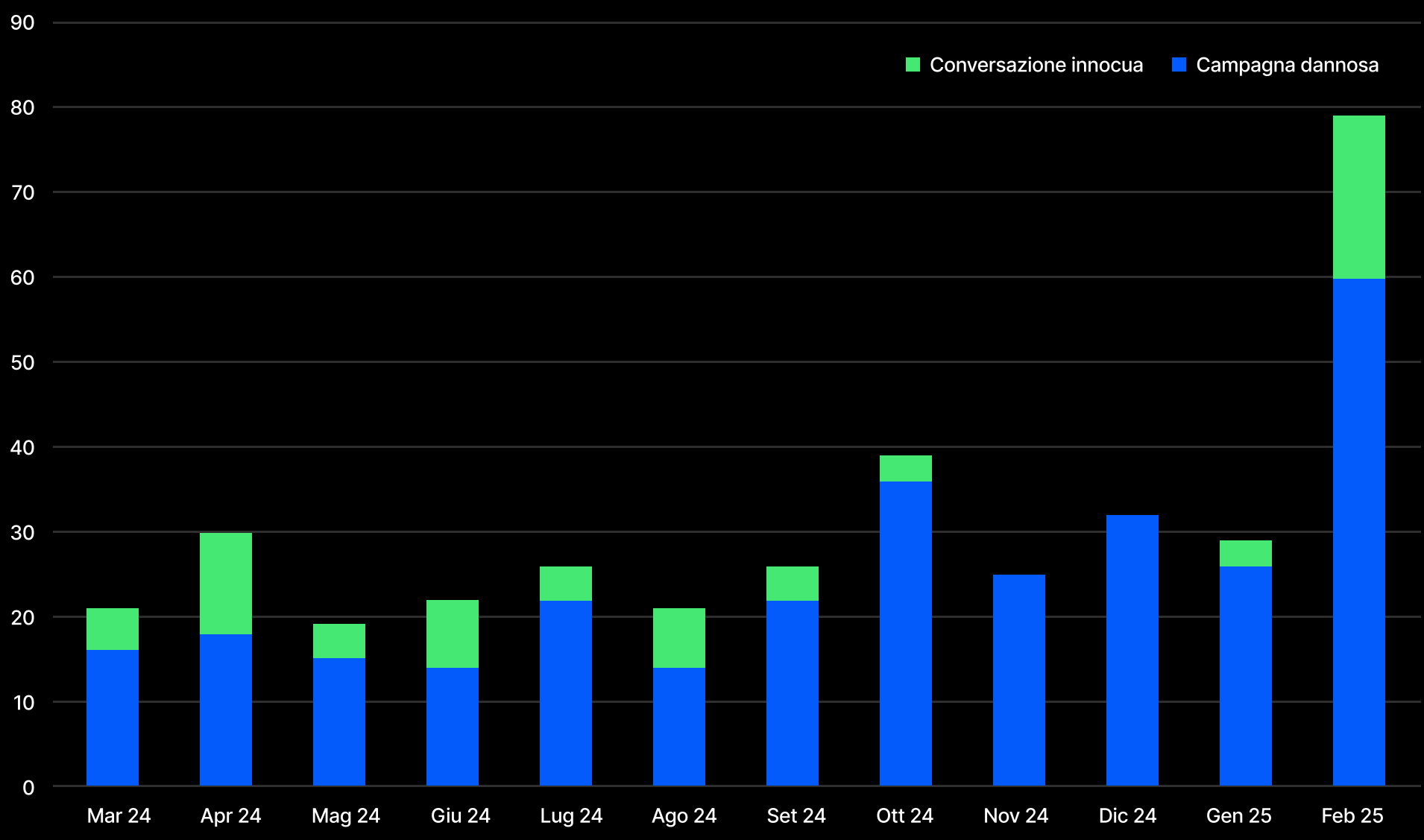
Proofpoint ha anche constatato che il criminale informatico iraniano TA453 utilizza tecniche simili basate su conversazioni innocue, spesso incentrate sulle questioni mediorientali.



Esca di TA427.

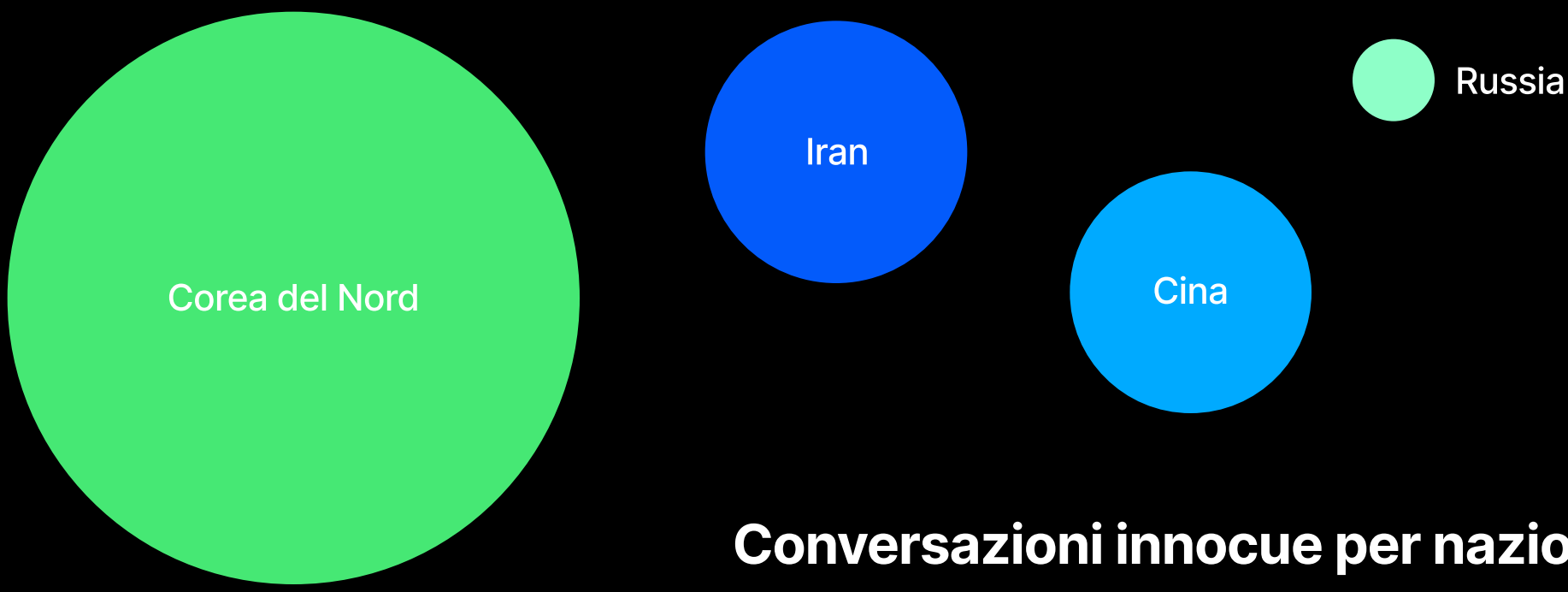
I dati provenienti dalle campagne sponsorizzate dagli Stati osservate durante l'anno scorso hanno messo in evidenza numerose tendenze, sia basate sui dati che aneddotiche. Come sottoinsieme di tutte le attività sponsorizzate dagli Stati osservate, le conversazioni innocue hanno rappresentato circa il 25% del totale delle campagne.

Campagne APT osservate nel tempo



Conversazioni innocue e campagne dannose osservate in un anno

Nel corso dell'anno scorso, i dati provenienti da tutte le campagne sponsorizzate dagli Stati osservate mostrano che la maggior parte delle conversazioni innocue provenivano da criminali informatici nordcoreani. Il criminale informatico TA427 ha utilizzato maggiormente le conversazioni innocue, rappresentando quasi il 70% di tutte le campagne APT che hanno utilizzato questa tecnica.



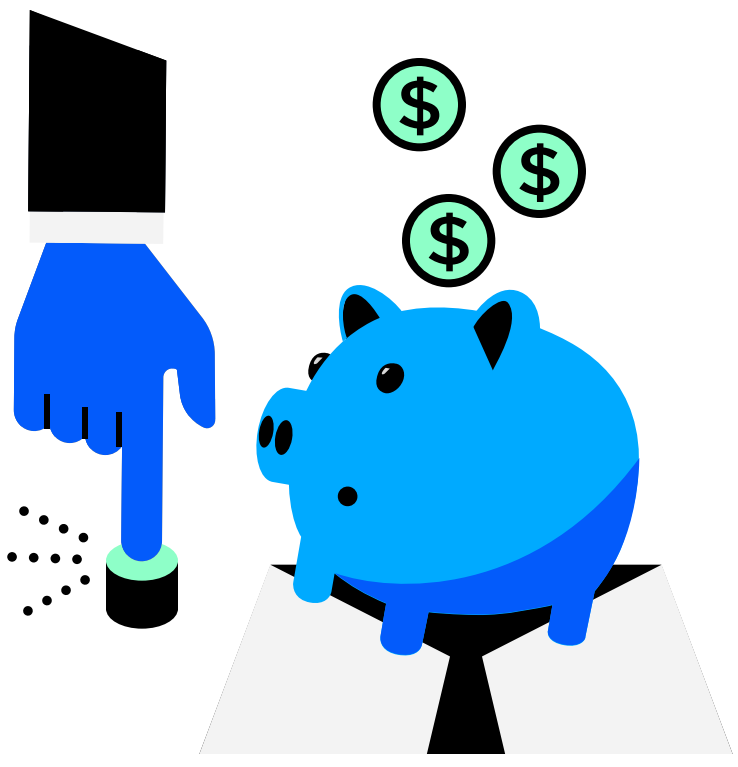
Conversazioni innocue per nazione

Argomenti comuni e tendenze

Mentre le campagne di TA427 hanno influenzato il set di dati, sono emerse numerose tendenze. Su circa 80 campagne che utilizzavano conversazioni innocue documentate dai ricercatori Proofpoint, oltre il 90% proveniva da mittenti la cui identità era stata rubata, incluse aziende e persone che vi lavoravano. Si trattava spesso di gruppi di riflessione, aziende governative nazionali o internazionali, mass media e istituti universitari.

I mittenti hanno preferito rubare l'identità di persone reali piuttosto che creare account email per collaboratori inesistenti presso le aziende interessate, probabilmente nel tentativo di rafforzare la credibilità delle loro esche. In numerosi casi, l'indirizzo del mittente imitava l'account personale di una persona piuttosto che il suo indirizzo email aziendale.

Un'altra interessante tendenza è la coerenza in termini di argomenti e oggetti delle conversazioni innocue. Oltre il 90% delle campagne sponsorizzate dagli Stati fingeva di essere interessate a collaborare e a farsi coinvolgere, che si trattasse di un invito a partecipare a un evento, una richiesta di commento a una notizia o una richiesta di incontro. Ciò che accomuna questi approcci è che il criminale informatico probabilmente cerca di ottenere una risposta elogiando la reputazione dell'obiettivo e richiedendo la sua competenza.



2. FBI. Internet Crime Report (Report sui crimini di Internet), 2024.
3. Chanalysis, "Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication" (Fatturato 2024 delle truffe delle criptovalute: il pig butchering aumenta di quasi il 40% in un anno mentre le frodi utilizzano l'IA e diventano sempre più sofisticate), febbraio 2025.

L'aumento del pig butchering

Per anni, i truffatori che utilizzano la tecnica del pig butchering, un tipo di frode basata su investimenti fittizi, hanno utilizzato conversazioni innocue per estorcere miliardi di dollari di criptovalute alle loro vittime. Questi truffatori utilizzano tecniche simili a quelle dei criminali informatici che utilizzano gli attacchi BEC. In generale, adescano i loro obiettivi con tecniche di social engineering sul lungo termine per poi indirizzarli su una piattaforma fasulla di investimento in criptovalute. Secondo l'ultimo report Internet Crime Report dell'FBI, le vittime hanno segnalato oltre 6,5 miliardi di dollari di perdite a causa di questo tipo di frodi legati agli investimenti[2].

Purtroppo, si basano su crimini reali, tra cui la tratta di esseri umani. Negli ultimi mesi, i truffatori specializzati nel pig butchering hanno esplorato anche aree più tradizionali come le frodi legate alle offerte di lavoro. Il fatturato proveniente dal pig butchering è aumentato del 40% nel 2024, con un aumento annuale del 210% del numero di depositi[3]. Per contro, l'ammontare medio dei depositi è diminuito, e i criminali informatici raccolgono un maggior numero di pagamenti, ma di importo significativamente inferiore.

Conclusione

Che commettano frodi o si dedichino allo spionaggio, i criminali informatici hanno tutti uno strumento comune nel loro arsenale. Invece dei cosiddetti attacchi tecnicamente sofisticati, i truffatori esperti utilizzano il social engineering. Sebbene temi e obiettivi variano, tutti hanno lo stesso obiettivo iniziale: far sì che le persone rispondano.

Secondo i dati di Proofpoint, nella maggioranza degli attacchi, le specifiche tecniche contano molto meno del fattore umano. Questo è il motivo per cui raccomandiamo le seguenti azioni per beneficiare di una difesa incentrata sulle persone.

Visibilità.

Devi identificare le vittime degli attacchi, i metodi utilizzati e se l'attacco è andato a segno. È importante conoscere il rischio individuale rappresentato da ogni utente: il modo in cui viene colpito, i dati a cui ha accesso e se tende facilmente a farsi trarre in inganno.

Rilevamenti ottimizzati dall'IA.

Le minacce di social engineering come gli attacchi TOAD e BEC sono in costante evoluzione. Scegli una piattaforma che integra la modellazione linguistica, in grado di riconoscere sottili modelli linguistici e indici comportamentali. In questo modo ti assicuri l'identificazione di queste minacce prima che possano causare danni.

Protezione contro il furto d'identità.

I tuoi team dovrebbero avere visibilità totale sui rischi come lo spoofing dei domini e la violazione degli account dei fornitori. Dovrebbero anche avere i controlli per contrastare le tattiche di furto d'identità, tra cui la capacità di mettere fuori servizio e eliminare i domini dannosi che imitano il tuo dominio.

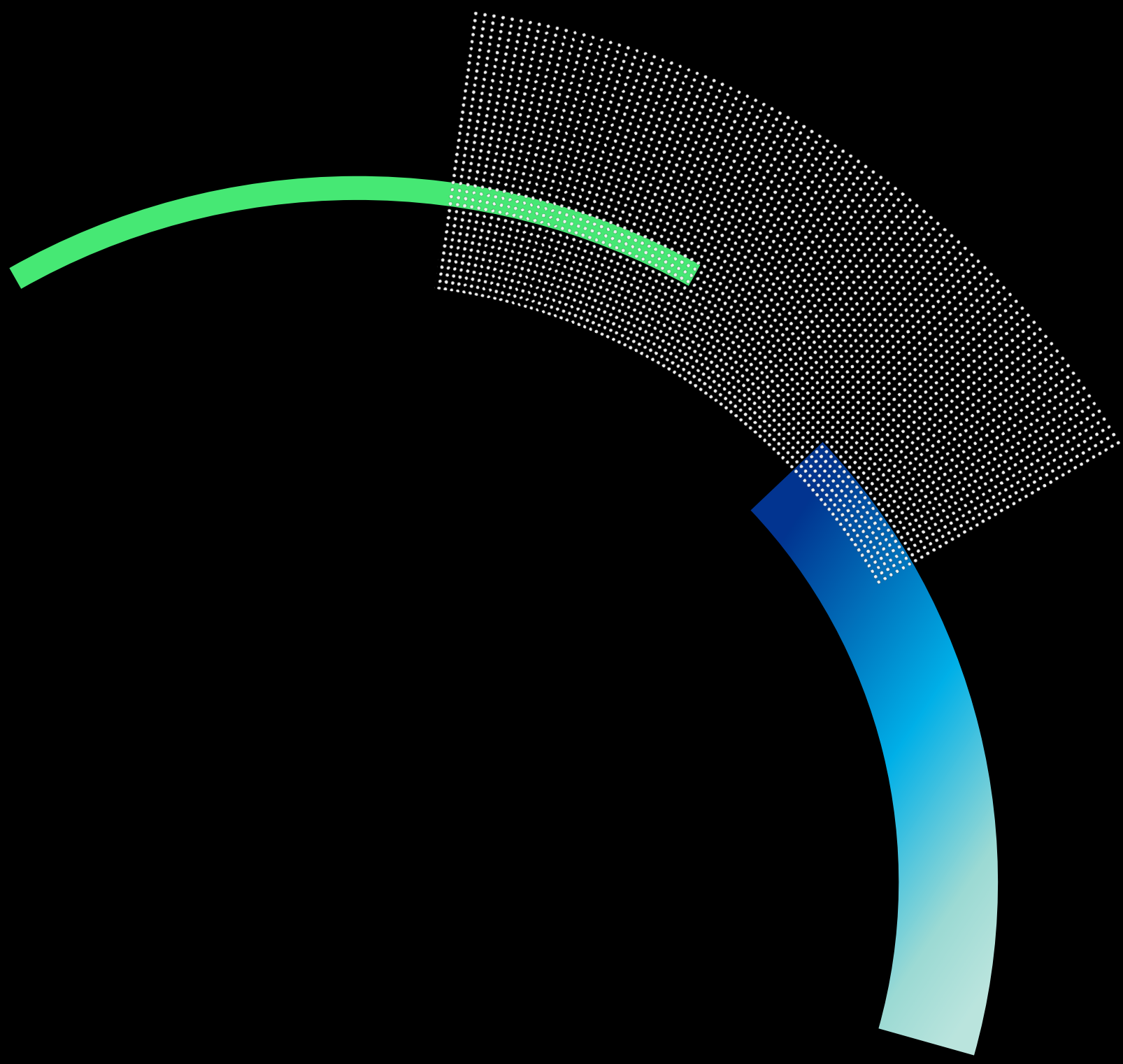
Sensibilizzazione personalizzata alla sicurezza informatica.

La formazione dovrebbe essere personalizzata e creata sulla base delle informazioni di threat intelligence più recenti. Inoltre, è essenziale fornire agli utenti avvisi contestuali e messaggi di formazione in tempo reale per aiutarli a prendere decisioni informate in termini di sicurezza.

Flussi di lavoro automatici.

Rilevamento delle minacce, neutralizzazione e risposta alle minacce dovrebbero essere automatizzati. Ciò riduce il volume delle minacce trasmesse via email su cui i team della sicurezza devono indagare.

Per saperne di più su come Proofpoint ti aiuta a valutare i rischi legati ai tuoi utenti e a ridurli, visita il sito proofpoint.com/it



proofpoint.

Proofpoint, Inc. è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui l'85% delle Fortune 100, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: www.proofpoint.com/it.

Seguici: LinkedIn

SCOPRI LA PIATTAFORMA PROOFPOINT →

[0400-016-05-01]