DER Faktor Mensch 2025

VOL. 1 | **SOCIAL ENGINEERING**

proofpoint®

Einleitung

Das gefährlichste Werkzeug eines Hackers ist wahrscheinlich kein schädlicher Link oder eine raffinierte Malware, sondern seine Fähigkeit, „Ihr Gehirn zu hacken“ – durch Nachahmen vertrauenswürdiger Personen sowie mit scheinbar harmlosen Gesprächen und glaubwürdigen Geschichten. Richtig eingesetzt, kann cleveres Social Engineering wesentlich effektiver sein als jede technische Attacke.

Social Engineering bezeichnet die Manipulation menschlicher Gefühle wie Angst, Ärger, Freude oder Stress mit dem Ziel, ein Opfer zu Aktionen zu verleiten, von denen der Betrüger profitiert. Von Angreifern geschickt gesteuert, tätigen Opfer beispielsweise einen Anruf, klicken auf einen Link oder laden eine Datei herunter.

Cyberangriffe auf Menschen sind meist mit einer Social-Engineering-Komponente verbunden, sei es eine Phishing-E-Mail, eine gefälschte Popup-Meldung auf einer kompromittierten Website oder ein scheinbar harmloser QR-Code auf einem Sticker. All das lässt sich einfacher personalisieren als je zuvor. Heute ist niemand mehr vor Angreifern sicher, da sie dank generativer KI nicht mehr durch Sprachen oder Standorte eingeschränkt sind.

Viele Kriminelle, die auf Business Email Compromise (BEC), Angriffe per Telefon (TOAD), Spionage und Pig Butchering-Betrug setzen, nutzen reines Social Engineering, um Personen zu Interaktionen zu bewegen. Durch die Wahl ihrer Taktiken vermeiden sie die Erkennung durch automatisierte Tools, die schädliche URLs und Anhänge identifizieren können.

Da die Social-Engineering-Methoden kontinuierlich weiterentwickelt werden, ist die Frage nach dem Schutz Ihrer Mitarbeiter berechtigt. Um die Resilienz von Angestellten gegenüber diesen Taktiken und das Ausmaß der Herausforderungen für Unternehmen zu verstehen, haben wir die Daten unserer eigenen Proofpoint Nexus®-Plattform für Bedrohungsdaten analysiert.

Wichtige Erkenntnisse

Top 5 der Social-Engineering-Taktiken:

1. **Provisionsbetrug**
2. **Erpressung**
3. **Angriff per Telefon (TOAD)**
4. **Aufgabe als Köder**
5. **Kostenvoranschlag**

25 %

Bei 25 % aller APT-Kampagnen kommt reines Social Engineering zum Einsatz.

90 %

Mehr als 90 % aller APT-Kampagnen mit reinem Social Engineering geben Interesse an Zusammenarbeit und Interaktionen vor.

50 %

Provisionsbetrug stieg im letzten Jahr um fast 50 %.

70 %

Erpressungsbetrug ging im letzten Jahr um fast 70 % zurück.

Informationen zu diesem Bericht

Bislang lieferte der *Bericht zum Faktor Mensch* einen umfassenden Überblick über personenzentrierte Bedrohungen, die in den vergangenen 12 Monaten von Proofpoint entdeckt, behoben und abgewehrt wurden. In diesem Jahr haben wir das Format geändert. Anstatt alle unsere Erkenntnisse in einem einzigen Bericht zusammenzufassen, stellen wir sie nun in einer mehrteiligen Reihe vor.

Dabei untersucht jeder Teil jeweils eine Bedrohungskategorie. Gleichzeitig zieht sich ein Thema durch alle Berichte: neue Entwicklungen in der Bedrohungslandschaft und die Gefährlichkeit aktueller Cyberangriffe durch die Kombination aus Technologie und Psychologie.

Daten-basis:

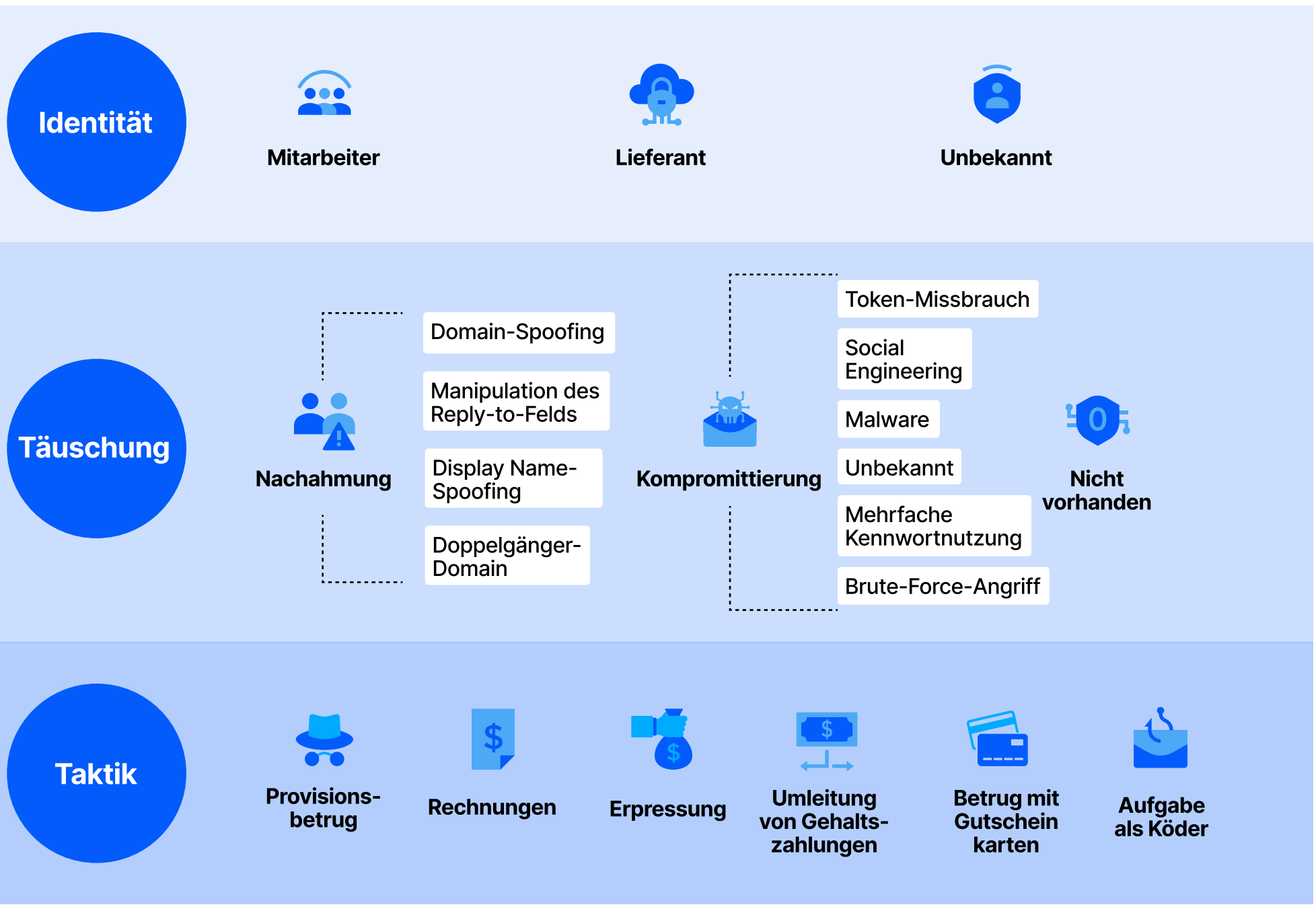
Dieser Bericht basiert auf Daten von Proofpoint-Bereitstellungen auf der ganzen Welt und damit auf einem der größten und vielfältigsten Datensätze in der Cybersicherheitsbranche. Jedes Jahr analysieren wir mehr als 3,4 Billionen E-Mails, 21 Billionen URLs, 0,8 Billionen Anhänge, 1,4 Billionen verdächtige SMS-Nachrichten und vieles mehr. Dabei stammen die Daten aus allen relevanten digitalen Kanälen.

** Zeitraum vom 1. März 2024 bis 28. Februar 2025.*

Unterschiede zwischen BEC und Betrug

Der Begriff Business Email Compromise (BEC) bezeichnet meist ein breites Spektrum an E-Mail-Betrugstaktiken, mit denen Kriminelle per Social Engineering jedes Jahr Milliarden US-Dollar stehlen. Laut dem aktuellen Internet Crime Report des FBI haben die Opfer in den letzten fünf Jahren mehr als 50 Milliarden US-Dollar durch Betrug verloren.[1]

Proofpoint interessiert sich für tiefergehende Details und hat über BEC hinaus die wichtigen Aspekte von E-Mail-Betrugsversuche – Social Engineering, finanziell motiviert und reaktionsbasiert – klassifiziert. Basierend darauf haben unsere Forscher die Taxonomie für E-Mail-Betrug entwickelt.



Proofpoint-Taxonomie für E-Mail-Betrug

1. FBI: *Internet Crime Report* (Bericht zu Internetkriminalität), 2024.

Basierend auf dieser Taxonomie entwickelte Proofpoint Erkennungsmaßnahmen, mit denen sich verschiedene Betrugstypen identifizieren und differenzieren lassen. Dadurch können unsere Forscher die gesamte Bedrohungslandschaft besser verstehen und sehen, welche Social-Engineering-Taktiken – einschließlich BEC – am häufigsten von Betrügern genutzt werden.

Trends bei **Betrugstaktiken**

Proofpoint Nexus erfasst jeden Monat mehr als 2 Milliarden potenziell schädliche E-Mails. Dabei erkennt und blockiert die Technologie reines Social Engineering mithilfe hochentwickelter Sprachanalysen und erreicht damit eine ähnliche Zuverlässigkeit wie bei technischen Angriffen wie Malware und Anmeldedaten-Phishing.

Unser Taxonomie-Regelsatz, der von Proofpoint-Analysten unter Einsatz von Machine Learning entwickelt wurde, erlaubt die weitergehende automatische Klassifizierung einiger dieser Aktivitäten mit Social-Engineering-bezogenen Tags. Diese Tags sind beispielsweise „Betrug mit Gutscheinkarten“, „Rechnungen“, „Umleitung von Gehaltszahlungen“, „Anfragen von Autoritätspersonen“ (wie CEO-Nachahmung), „Geldkuriere“ und viele andere.

Nach dem Filtern unserer kompletten Erkennungsdaten mithilfe spezifischer Tags für bekannte Betrugstypen zeigte sich, dass folgende Social-Engineering-Taktiken am häufigsten auftraten:

Provisionsbetrug

Ein Angreifer verspricht eine beträchtliche Geldsumme oder wertvolle Artikel als Gegenleistung für einen kleinen Geldbetrag, den ihm das Opfer senden soll.

Erpressung

Ein Angreifer droht dem Opfer mit physischer Gewalt oder Rufschädigung, wenn es seinen Forderungen nicht Folge leistet. Das ist der wichtige Unterschied zwischen Ransomware-basiertem Datendiebstahl und Erpressung.

Angriffe per Telefon (TOAD)

Ein Angreifer versucht, die Zielperson zum Anrufen bei einer Telefonnummer zu verleiten, die in der Nachricht als Text, Bild oder Anhang enthalten ist. Wenn das Opfer dort anruft, wird es dazu gebracht, eine Remote-Zugriffs-Software zu installieren oder anderweitig mit schädlichen Inhalten zu interagieren. Proofpoint blockiert jedes Jahr 117 Millionen TOAD-Nachrichten.

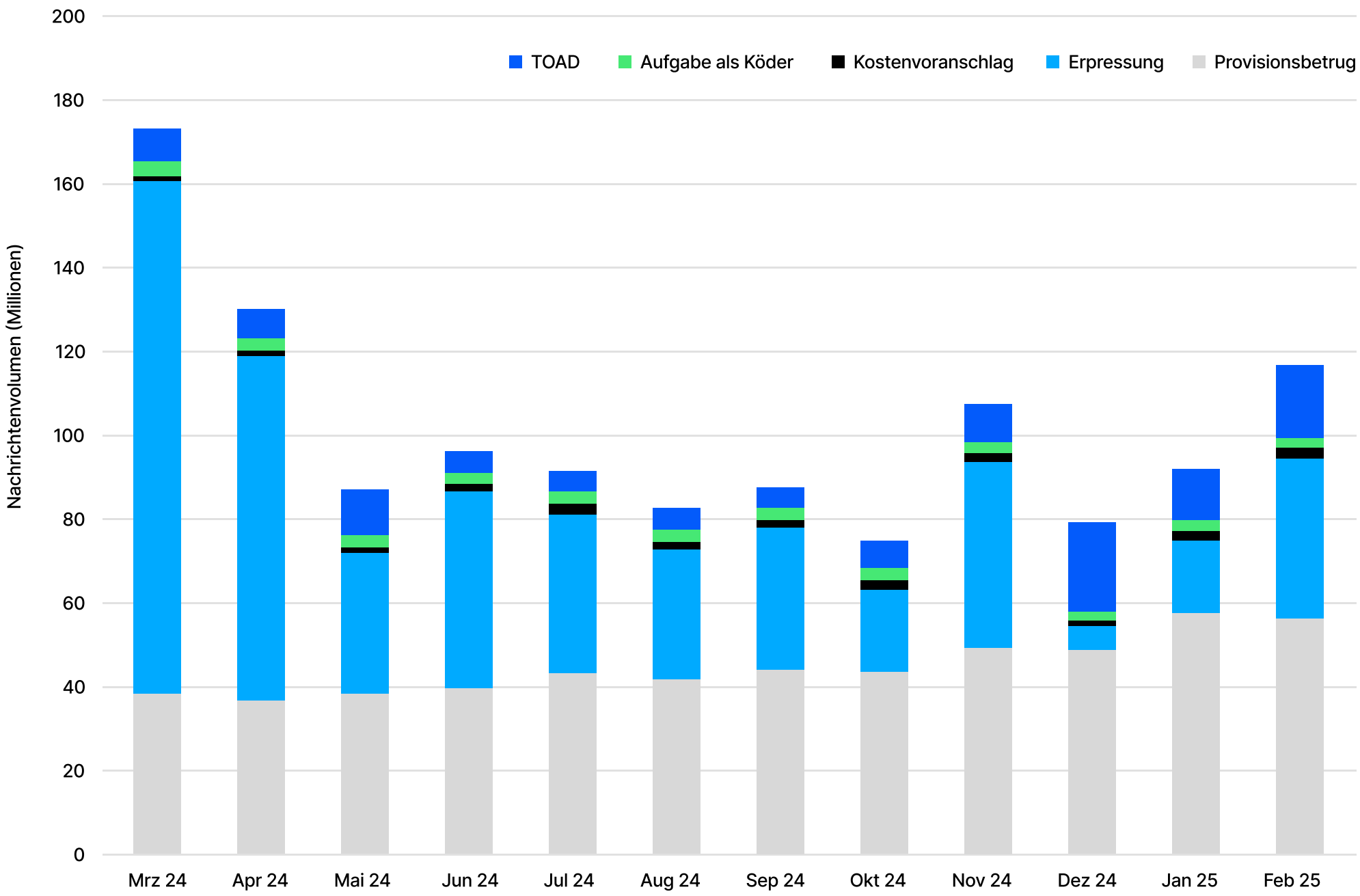
Aufgabe als Köder

Ein Angreifer stellt keine konkrete Forderung, sondern bittet das Opfer darum, ihn zu kontaktieren, um eine bestimmte Aufgabe zu erfüllen, z. B. einen Einkauf durchzuführen.

Kosten-voranschlag

Ein Angreifer sendet eine Fake-Bitte um ein Angebot, das zu Finanzdiebstahl oder Folgeaktivitäten wie Malware, Anmeldedaten-Kompromittierung oder dem Diebstahl physischer Güter führen kann.

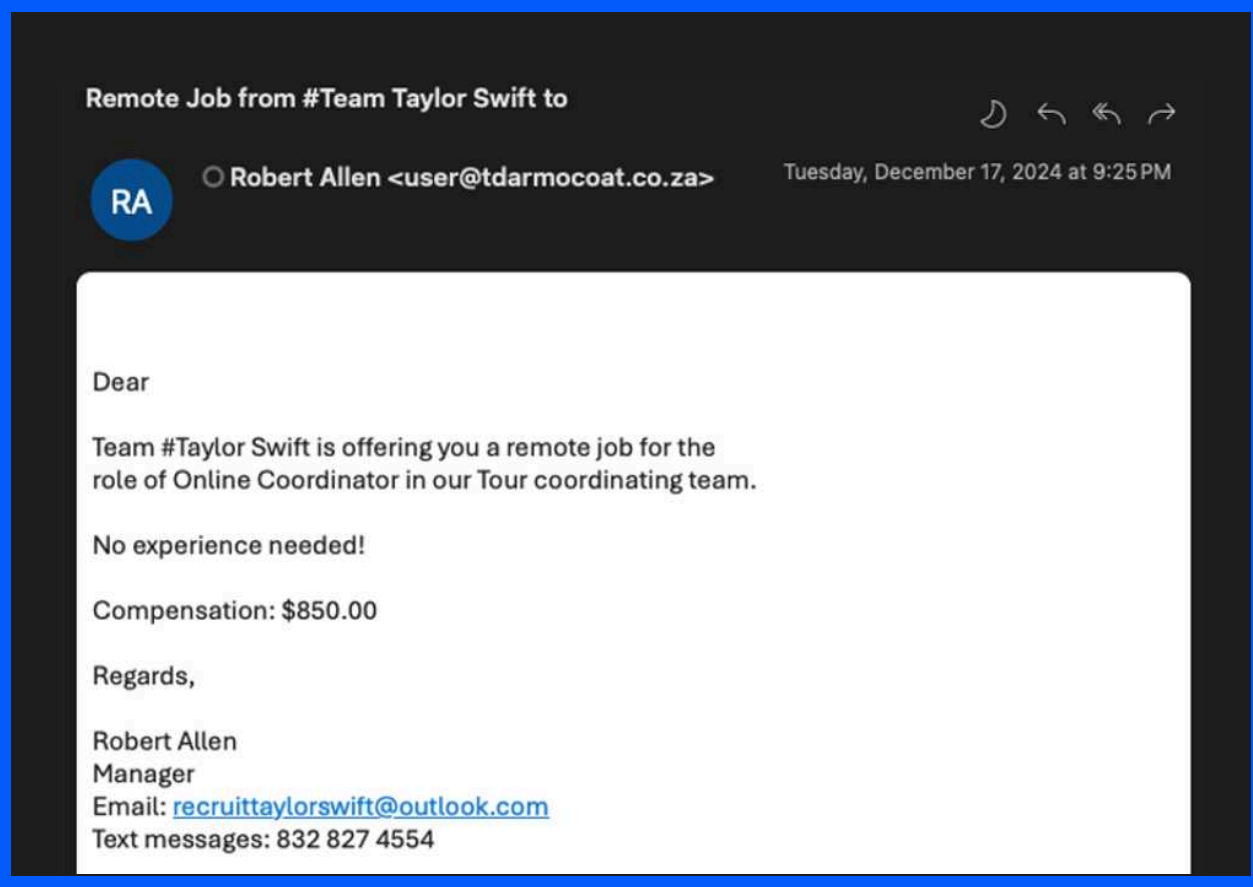
Am häufigsten beobachtete BEC-Taktiken



Top 5 der Social-Engineering-Taktiken, die vom BEC-Modul von Proofpoint Nexus identifiziert wurden

Auffällig ist, dass mit Erpressung verbundene Betrugsversuche insgesamt abnehmen. Zwischen März 2024 und Februar 2025 gingen diese Bedrohungen um mehr als 68 % zurück – von 122 Millionen auf 38 Millionen pro Monat. Währenddessen nahm Provisionsbetrug im gleichen Zeitraum um 47 % von 38 Millionen auf 56 Millionen zu. Grund hierfür können die abnehmende Effektivität von Erpressungstaktiken oder die Verbesserungen von E-Mail-Anbietern zur Abwehr dieser konkreten Bedrohungen sein, die stes stets auf die gleiche Weise enden: mit gestohlenem Geld.

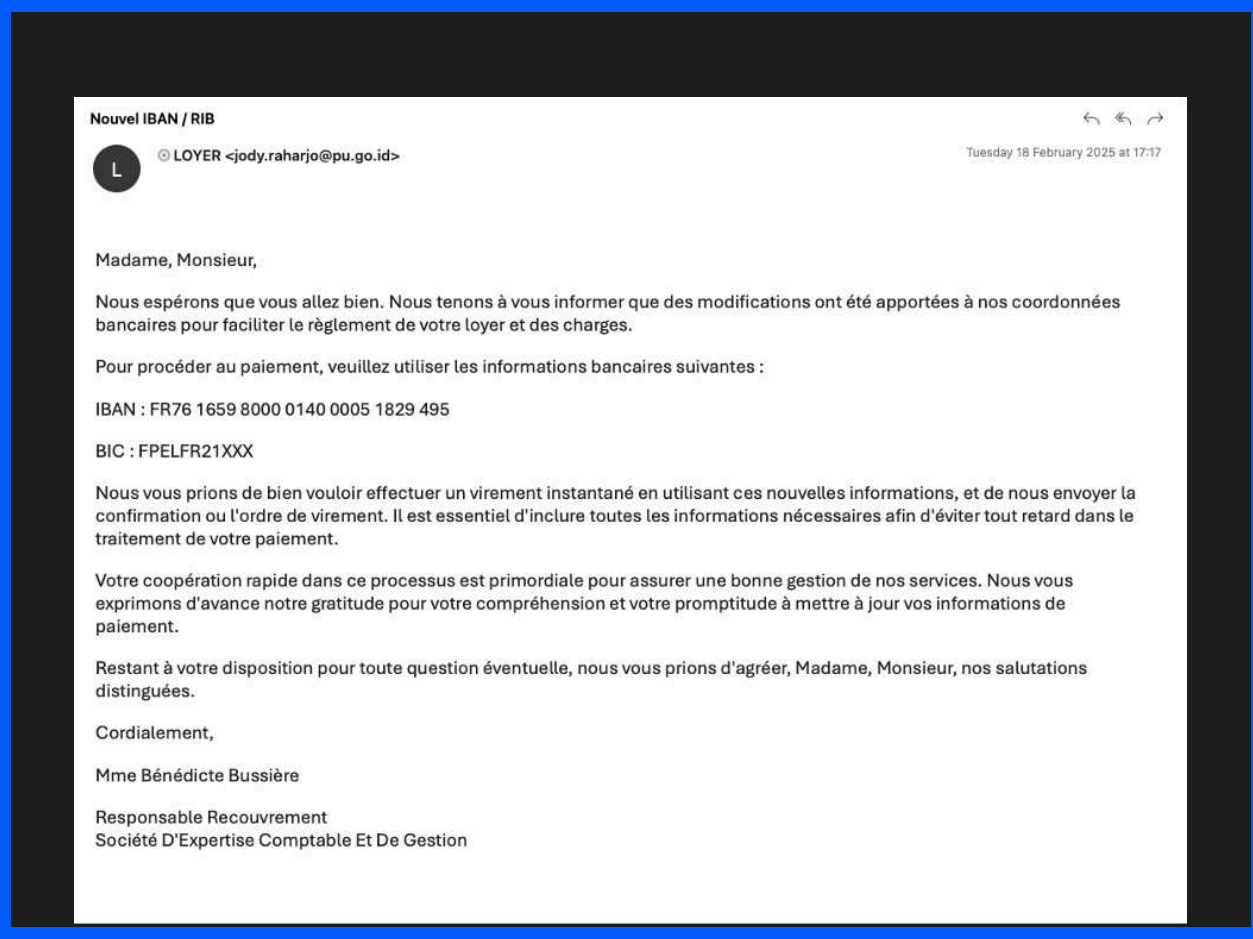
Nicht alle Betrugsversuche sehen jedoch gleich aus. So nutzen Provisionsbetrüger auch ungewöhnliche E-Mail-Köder wie „Klavier zu verkaufen“ oder Jobangebote, um arglose Opfer zu Interaktionen zu verleiten. Im Dezember 2024 fanden Forscher sogar Provisionsbetrüger, die gefälschte Jobangebote für die „Eras“-Tour von Taylor Swift verschickten. Aufmerksame Empfänger wurden natürlich sofort misstrauisch, doch bei anderen lösten diese E-Mails eine solche Begeisterung aus, dass einige Personen darauf hereinfielen.



Fake-E-Mail für Jobangebot zu Taylor Swift-Tour

Ein **weltweites** Problem

Auch wenn unsere Forscher überwiegend auf Englisch abgefasste Betrugsversuche beobachten, findet Proofpoint durchaus betrügerische Nachrichten in anderen Sprachen. So sendet beispielsweise der Betrüger TA2900 E-Mails in französischer Sprache mit Mietzahlungsthemen, um Menschen in Frankreich und gelegentlich auch in Kanada anzugreifen.



Phishing-E-Mail mit Mietzahlungsbetrug

Bei diesen Kampagnen, die Proofpoint mehrmals pro Woche beobachtet, wird den Empfängern erklärt, dass die Bankkontodaten des Vermieters sich geändert hätten und die nächste Mietzahlung an ein neues, vom Angreifer angegebenes Konto überwiesen werden soll. Interessant ist dabei, dass diese E-Mails ungewöhnliche Ausdrucksweisen und E-Mail-Inhalte aufweisen, die eine Erstellung per KI nahelegen.

Da generative KI sich immer stärker durchsetzt, werden Bedrohungsakteure den Kreis ihrer Ziele erweitern können, indem sie ihr Social Engineering besser an bestimmte Orte und Sprachen anpassen. Fakt ist jedoch, dass es für die Erkennung dieser Bedrohungen keine Rolle spielt, ob sie von Menschen oder einer KI verfasst wurden.

Harmlose Konversation

Social Engineering dreht sich darum, eine Person unvorsichtig werden zu lassen. Das lässt sich zum Beispiel dadurch bewerkstelligen, dass der Angreifer sein Gegenüber mit einer harmlosen Nachricht anspricht und in ein längeres Gespräch verwickelt. Das schafft Vertrauen und bringt das Opfer dazu, nach längeren und scheinbar vertrauenswürdigen Interaktionen mit dem Angreifer unvorsichtig zu werden.

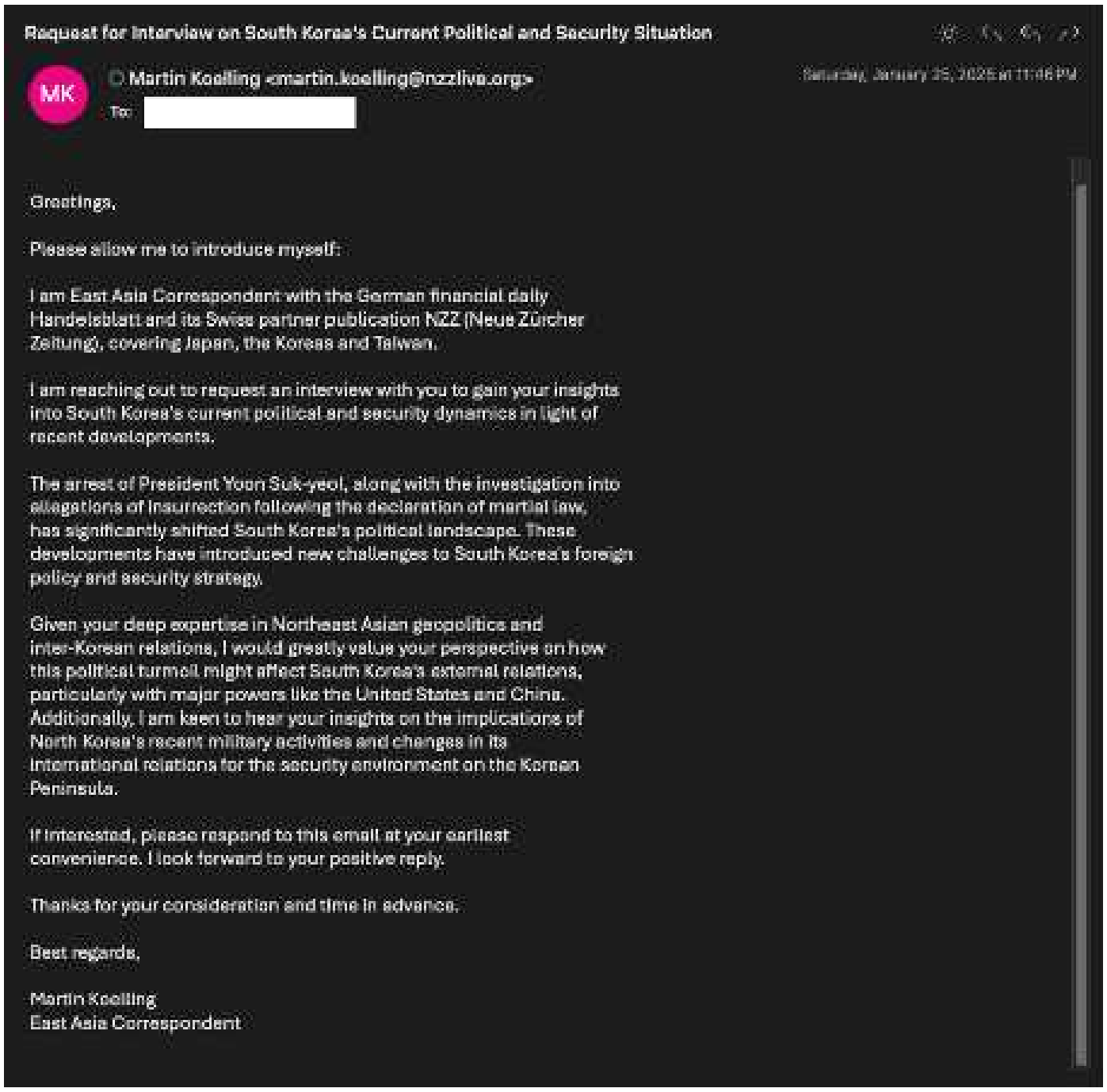
Sobald der Angreifer ein Vertrauensverhältnis aufgebaut hat, fasst er mit weiteren E-Mails nach. Da die Zielperson jetzt eher zu Interaktionen geneigt ist, enthalten diese Nachrichten schädliche Links oder Anhänge. Bedrohungsakteure nutzen auch harmlose Konversation, um die Reaktion zu testen und festzustellen, ob das Opfer zu Interaktionen bereit ist. Dadurch vermeiden sie, dass ihre Malware oder eine Infektionskette nutzlos „verbrennt“, da sie erkannt und blockiert wurde.

Schwerpunkt APT

Für staatlich unterstützte Akteure ist Spionage weiterhin die größte Motivation. Daher werden harmlose Konversationen bei Phishing-Kampagnen von APT-Akteuren (Advanced Persistent Threat) genutzt. Diese Konversationen dienen nicht nur als Köder, um Informationen über Außenpolitik oder aktuelle Ereignisse zu erhalten, sondern können den Akteuren auch Einblicke in die Position einer Regierung oder Entscheidungs-findungsprozesse bei politischen Problemen verschaffen. Diese Erkenntnisse ermöglichen es den staatlichen Unterstützern der Akteure, ihre eigene Politik und entsprechende Reaktionen anzupassen.

So kommuniziert der nordkoreanische Bedrohungsakteur TA427 über einen Zeitraum von jeweils mehreren Wochen oder Monaten mit seinen Zielpersonen und nutzt dabei harmlose Konversationen. Der Akteur tauscht die gefälschten Absender regelmäßig aus, interagiert jedoch mit seinen Zielpersonen stets zu den gleichen Themen, die sich häufig um aktuelle Ereignisse auf der koreanischen Halbinsel drehen. Im Januar 2025 imitierte TA427 einen Journalisten, der Details darüber suchte, wie der Umsturzversuch und die nachfolgende Verhaftung des früheren südkoreanischen Präsidenten Yoon Suk Yeol sich auf die Sicherheits- und Außenpolitik Südkoreas auswirken würde.

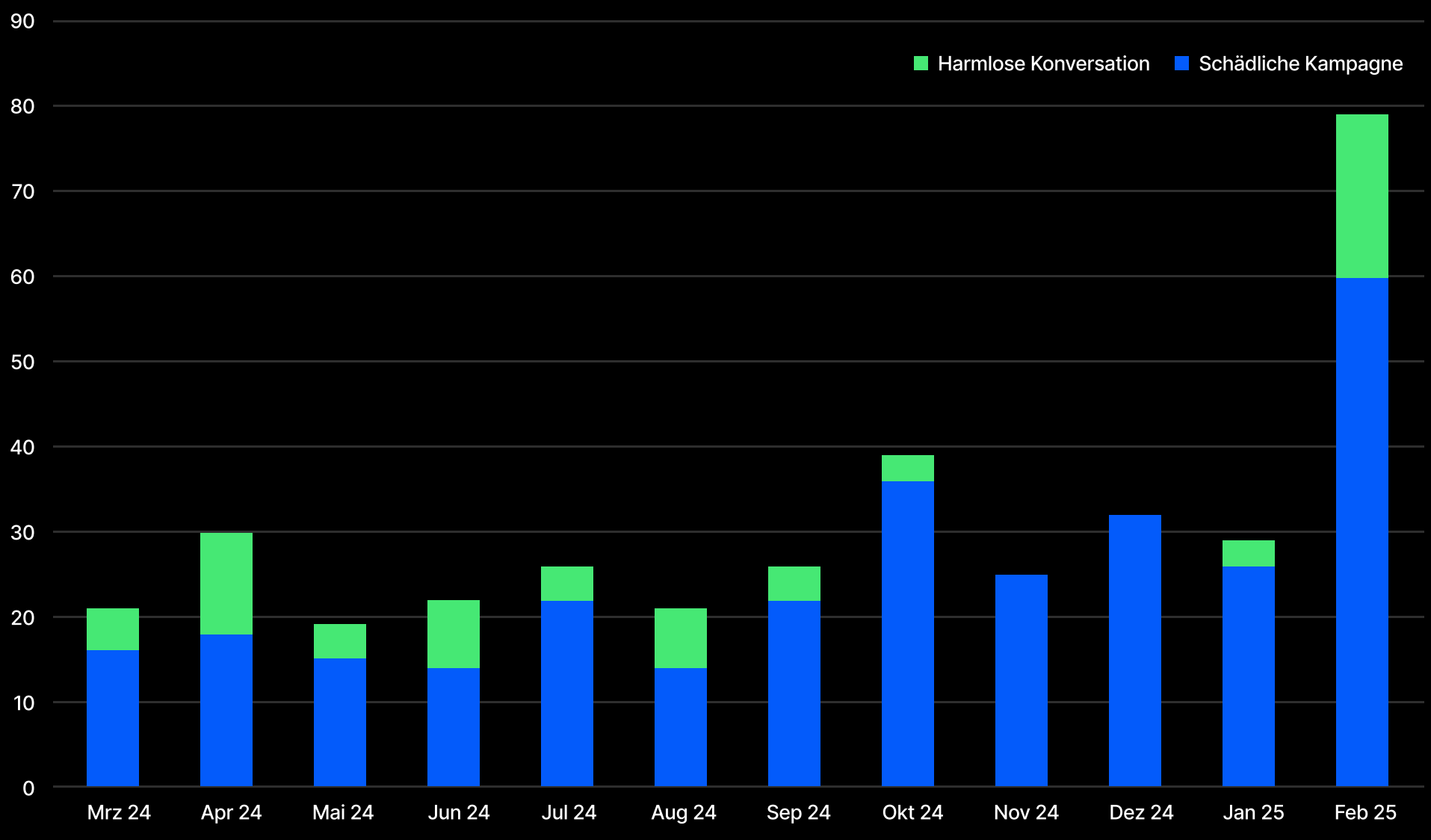
Wie Proofpoint beobachten konnte, nutzt der iranische Bedrohungsakteur TA453 ähnliche Techniken (allerdings oft mit Fokus auf die Politik im Nahen Osten).



Köder von TA427

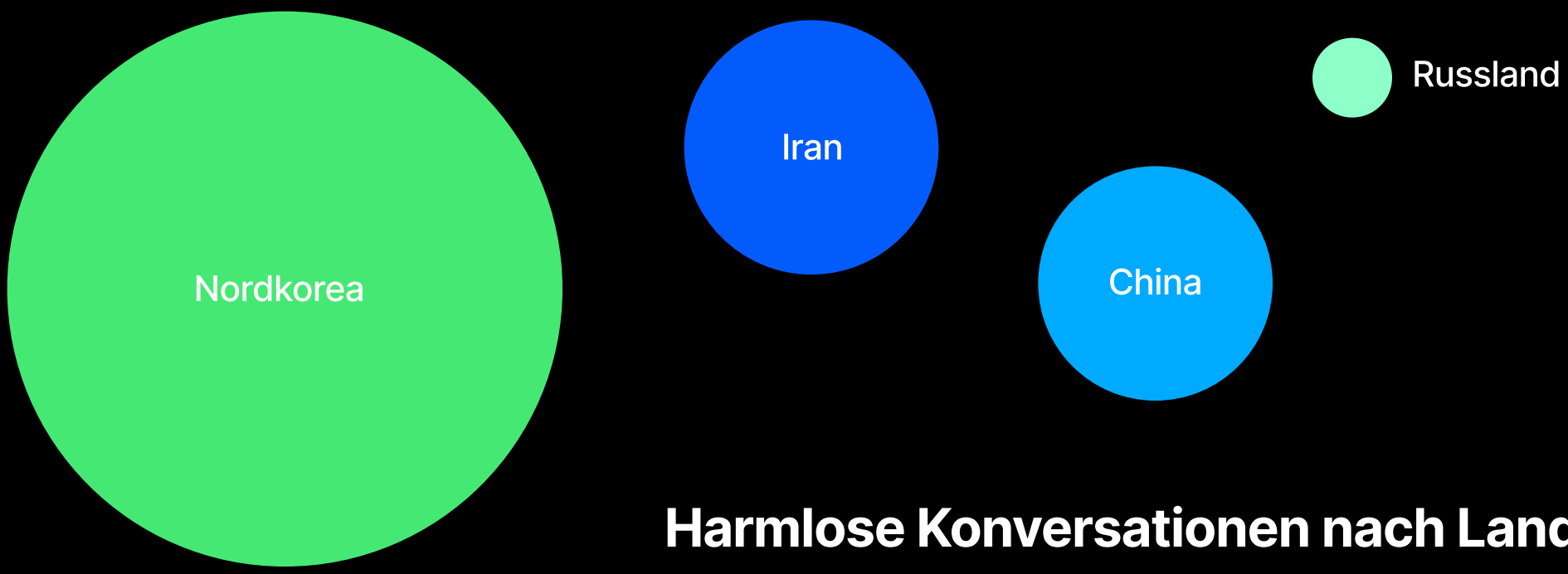
Die anekdotischen und datenbasierten Beobachtungen staatlich unterstützter Kampagnen im letzten Jahr zeigten mehrere Trends auf. Die hier thematisierten harmlosen Konversationen als Teil staatlich unterstützter Aktivitäten hatten einen Anteil von etwa 25 % aller Kampagnen.

APT-Kampagnen im Zeitverlauf



Harmlose Konversation im Vergleich zu schädlichen Kampagnen im Verlauf eines Jahres

Im Verlauf des letzten Jahres zeigten die Daten aller beobachteten staatlich unterstützten Kampagnen, dass die meisten harmlosen Konversationen von nordkoreanischen Akteuren stammten. Dabei tat sich TA427 besonders hervor – mit fast 70 % aller APT-Kampagnen, die diese Technik nutzten.



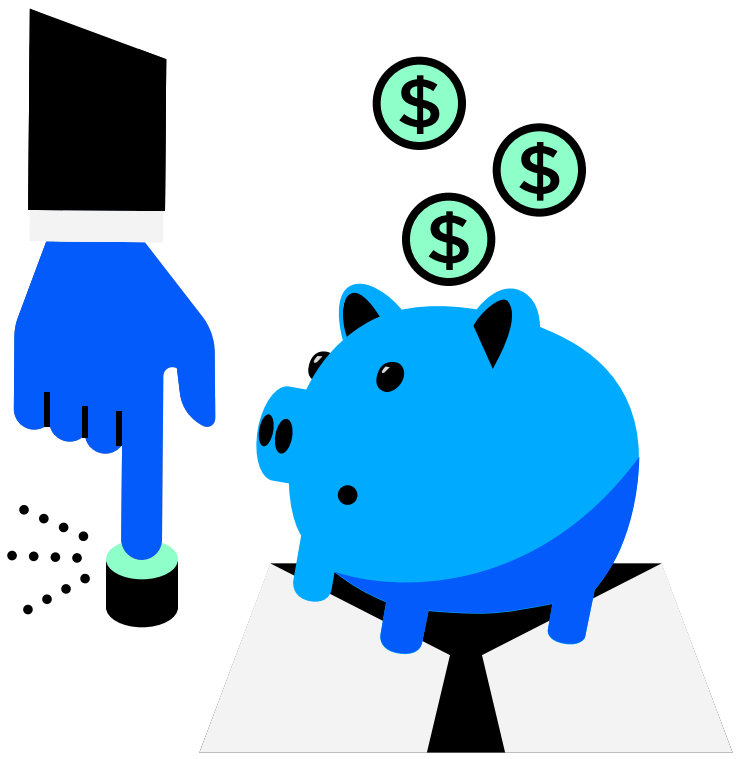
Harmlose Konversationen nach Land

Gängige Themen und Trends

Auch wenn die Kampagnen von TA427 den Datensatz stark beeinflussten, zeigten sich einige Trends. Bei etwa 80 Kampagnen mit harmlosen Konversationen, die von Proofpoint-Forschern dokumentiert wurden, stammten mehr als 90 % von gefälschten Absendern. Dabei handelt es sich oft um Think Tanks, nationale oder internationale Regierungsbehörden, Medienunternehmen sowie akademische Einrichtungen (bzw. deren Mitarbeiter).

Die Absender fälschten regelmäßig eher echte Personen, anstatt E-Mail-Konten für Fake-Personen bei den gefälschten Organisationen zu erstellen – wahrscheinlich um ihre Köder möglichst glaubwürdig erscheinen zu lassen. In mehreren Fällen fälschten die Absender das private Konto einer Person statt ihrer beruflichen E-Mail-Adresse.

Ein weiterer interessanter Trend ist die Konsistenz des Themas und die Nutzung scheinbar harmloser Konversationsansätze. Mehr als 90 % der staatlich unterstützten Kampagnen gaben vor, an Zusammenarbeit und Interaktionen interessiert zu sein. Das konnte die Einladung zu einem Event, die Bitte um einen Kommentar zu einer Nachrichtenmeldung oder aber die Bitte um ein Treffen sein. All diese Ansätze haben gemeinsam, dass der Angreifer es auf eine Reaktion abgesehen hat, indem er die Reputation der Zielperson lobt und ihre Expertise einholen will.



Pig Butchering nimmt zu

Jahrelang nutzten Pig Butchering-Betrüger harmlose Konversationen, um Menschen um Milliarden Dollar an Kryptowährung zu betrügen. Dabei griffen sie auf ähnliche Techniken wie BEC-Akteure zurück. Meist köderten sie sie ihre Ziele in langen Social-Engineering-Interaktionen und brachten sie schließlich dazu, in eine gefälschte Kryptowährungsplattform zu investieren. Laut dem aktuellen Internet Crime Report des FBI meldeten die Opfer mehr als 6,5 Milliarden US-Dollar Schäden durch Investment-Betrug.[2]

Leider stehen diese Aktivitäten mit Verbrechen in der realen Welt (wie Menschenhandel) in Verbindung. In den letzten Monaten dehnten diese Betrüger ihr Spektrum auf klassische betrügerische Taktiken wie Betrug mit Stellenanzeigen aus. Die durch Pig Butchering erzielten Umsätze stiegen im Jahr 2024 um 40 %, wobei die gesamte Geldsumme pro Jahr um 210 % stieg.[3] Interessant ist, dass der durchschnittliche Geldbetrag pro Zahlung zurückging, die Bedrohungsakteure aber wesentlich mehr Zahlungen erhielten.

2. FBI: *Internet Crime Report* (Bericht zu Internetkriminalität), 2024.
3. Chanalysis: *Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication* (Umsätze durch Kryptobetrug 2024: Pig Butchering nimmt im Jahresvergleich um 40 % zu, da die Betrugsindustrie auf KI setzt und raffinierter wird), Februar 2025.

Fazit

Unabhängig davon, ob Bedrohungsakteure es auf Betrug oder Spionage abgesehen haben, gehört ein Tool üblicherweise zu den Standardwerkzeugen: Social Engineering. Auch wenn sich die Themen und Ziele unterscheiden, wollen sie alle das Gleiche: die angegriffenen Personen zu bestimmten Reaktionen verleiten.

Die Daten von Proofpoint zeigen, dass bei den meisten Angriffen die technischen Faktoren eine deutlich geringere Rolle spielen als der Faktor Mensch. Deshalb empfehlen wir die Implementierung von personenzentriertem Schutz.

Transparenz

Sie müssen wissen, wer wie angegriffen wird und ob die angegriffene Person reagiert hat. Dabei müssen Sie das individuelle Risiko der einzelnen Anwender berücksichtigen, einschließlich der Informationen dazu, wie sie angegriffen werden, auf welche Daten sie zugreifen können und wie leicht sie sich täuschen lassen.

KI-gestützte Erkennung

Social-Engineering-Bedrohungen wie TOAD und BEC werden ständig weiterentwickelt. Wählen Sie daher eine Plattform mit integrierten Sprachmodellen, die subtile Sprachmuster und Indikatoren für Verhaltensweisen identifizieren kann. Dadurch lassen sich diese Bedrohungen identifizieren, bevor sie Schaden anrichten können.

Schutz vor Nachahmern

Ihre Teams sollten einen kompletten Überblick über Risiken wie Domain-Spoofing und kompromittierte Lieferantenkonten haben und über Kontrollen verfügen, mit denen sich Nachahmungstaktiken abwehren lassen – einschließlich der Möglichkeit zur Stilllegung und Beseitigung böswilliger Doppelgänger Ihrer Domain.

Maßgeschneiderte Sicherheitsschulungen

Schulungen sollten personalisiert sein und die neuesten Bedrohungsdaten nutzen. Wenn Ihre Mitarbeiter kontextbezogene Warnungen und Echtzeit-Hinweise erhalten, können sie informierte Sicherheitsentscheidungen treffen.

Automatisierte Workflows

Die Erkennung, Behebung und Abwehr von Bedrohungen sollte automatisch erfolgen, damit das Team deutlich weniger E-Mail-Bedrohungen untersuchen muss.

Weitere Informationen dazu, wie Sie dank Proofpoint die personenzentrierten Risiken Ihres Unternehmens identifizieren und beheben können, finden Sie unter www.proofpoint.de.

proofpoint.

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 85 Prozent der Fortune 100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter www.proofpoint.de.

Verbinden Sie sich mit Proofpoint: LinkedIn

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →

0400-016-04-01]