proofpoint.

Die Fakten zu Social Engineering

Aufräumen mit den typischen Missverständnissen

Je mehr Sie über Ihre Mitarbeiter, deren Schwächen und Berechtigungen sowie die Bedrohungsakteure wissen, desto besser können Sie Social-Engineering-Angriffe abwehren. Doch während wir beim Identifizieren potenzieller Bedrohungen immer besser werden, entwickeln auch die Cyberkriminellen ihre Methoden weiter und verhalten sich auf unvorhergesehene Weise.

Damit Sie ihnen einen Schritt voraus bleiben, stellen wir hier die neuesten Trends, Verhaltensweisen und typischen Missverständnisse über Bedrohungsakteure und ihre Angriffstaktiken vor.

Missverständnis 1

Bedrohungsakteure setzen bevorzugt auf überfallartige Angriffe

Die Realität:

Cyberkriminelle investieren häufig viel Zeit in Recherchen und bauen Vertrauen auf, bevor sie zuschlagen.

TA453

TA453, eine Gruppe mit Iran-Bezug, nutzt für ihre Kampagnen oft harmlose Konversationen, um Informationen von ihren Zielen zu erhalten.

TA406

Die nordkoreanische Gruppe TA406 sucht nach den Anmeldedaten der Opfer sowie weiteren Informationen, bevor sie schädliche Links oder Anhänge verschickt.

TA499

TA499, ein Bedrohungsakteur mit Russland-Bezug, versuchte mit scheinbar harmlosen E-Mails, vor der Durchführung von Angriffen Informationen von hochrangigen Mitarbeitern zu erlangen.

Missverständnis 2

Die Nutzung seriöser Services wie Google und Microsoft ist sicher

Die Realität:

Bedrohungsakteure missbrauchen regelmäßig seriöse Services, um Anmeldedaten zu erfassen sowie Malware zu hosten und zu verteilen.

14 %

14 % aller beobachteten schädlichen Kampagnen nutzten seriöse Services aus.

Von Google gehostete URLs wurden am häufigsten missbraucht…

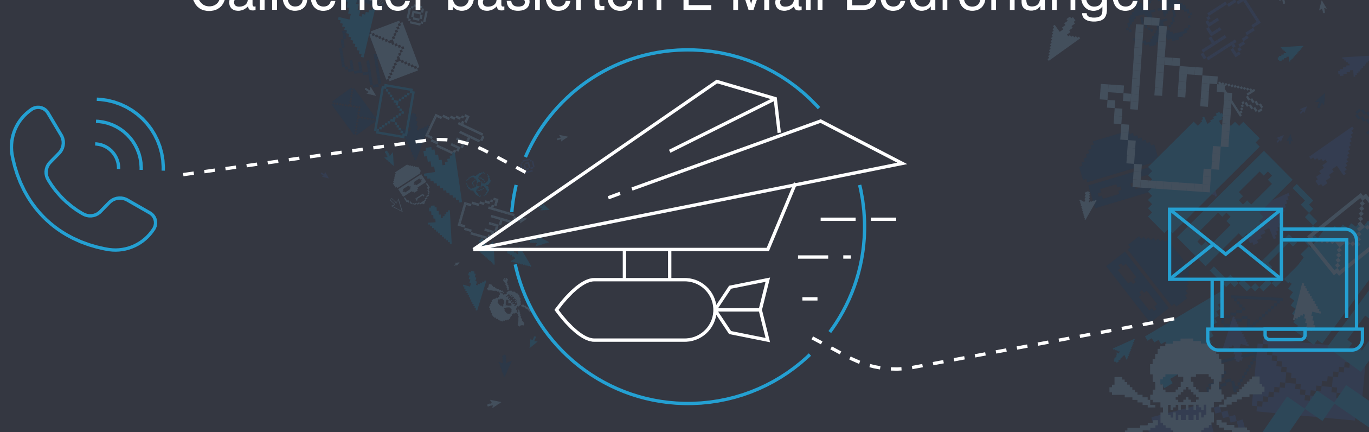
…aber von Microsoft gehostete URLs wurden fast zweimal so häufig angeklickt wie Google-URLs.

Missverständnis 3

Bedrohungsakteure setzen ausschließlich auf E-Mails

Die Realität:

Die branchenweit führenden Bedrohungsanalysen von Proofpoint entdecken immer häufiger Angriffe mit Callcenter-basierten E-Mail-Bedrohungen.



250.000

Proofpoint beobachtet täglich mehr als 250.000 Telefonangriffe (TOAD).

TOAD-E-Mails enthalten keine Links oder Anhänge, sondern fordern die Empfänger auf, selbst ein falsches Callcenter anzurufen.

50.000 USD

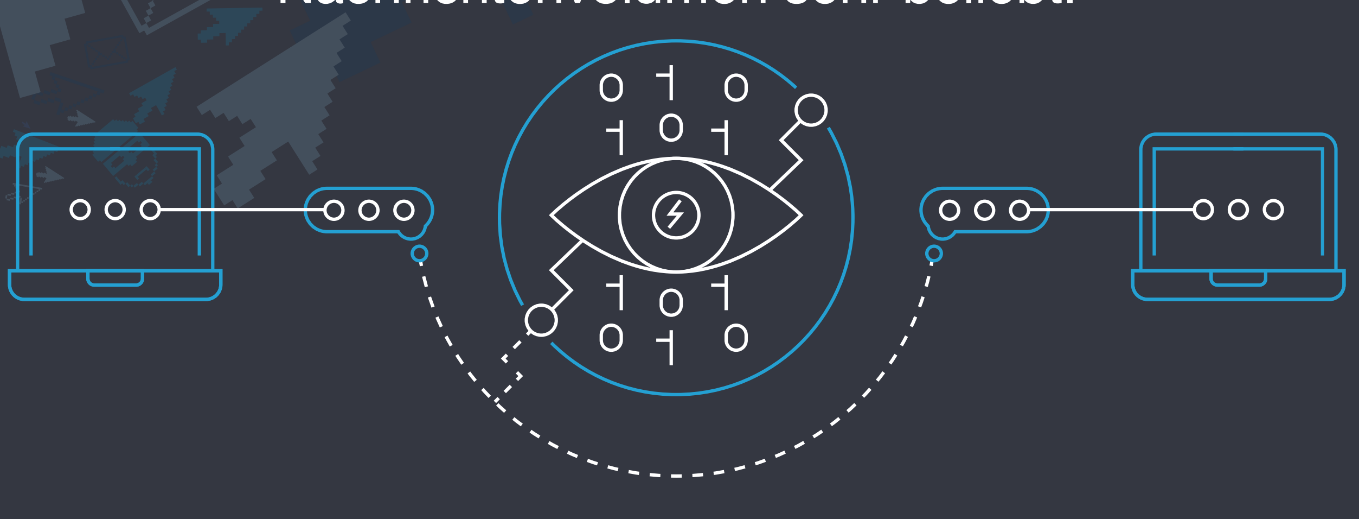
In einem Fall verlor ein Opfer bei einem TOAD-Angriff fast 50.000 USD.

Missverständnis 4

Interne Konversationen sind stets sicher

Die Realität:

Thread-Hijacking bzw. die Übernahme von Gesprächen ist bei einigen finanziell motivierten Angreifern mit hohem Nachrichtenvolumen sehr beliebt.



500

Proofpoint beobachtete mehr als 500 Kampagnen, die auf Thread-Hijacking setzten…

16

…und 16 verschiedene Malware-Familien verteilten…

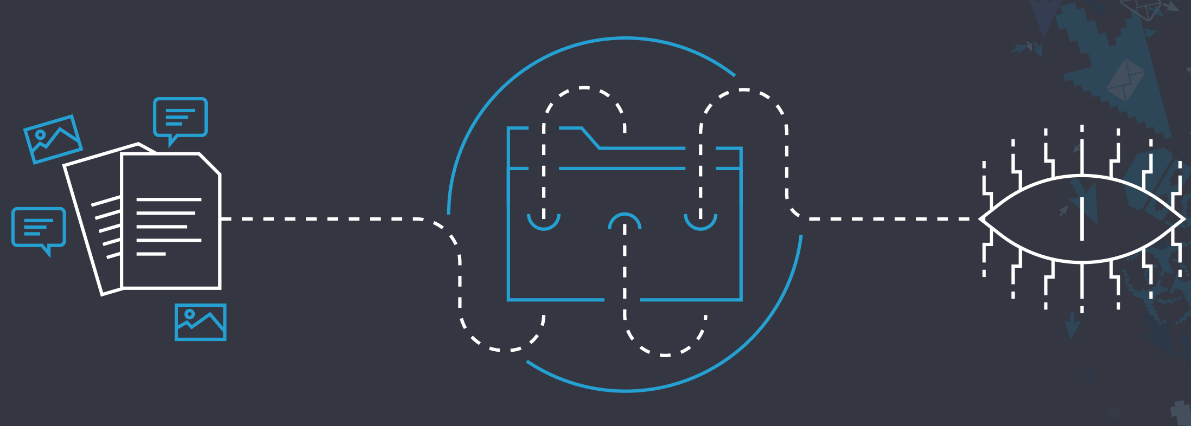
…darunter Qbot, Emotet, IcedID und Racoon Stealer.

Missverständnis 5

Bedrohungsakteure nutzen ausschließlich standardisierte geschäftsbezogene Inhalte

Die Realität:

Cyberkriminelle nutzen aktuelle Events, Nachrichten, Popkultur und vieles mehr, um die Interaktion mit schädlichen Inhalten zu steigern.



Im Jahr 2021 beobachtete Proofpoint jeden Monat hunderte Millionen COVID-bezogene Köder.

Steuerbezogene Themen, die Steuersenkungen im Austausch für vertrauliche Informationen anbieten, sind bei Cyberkriminellen beliebt.

Andere beobachtete Köder sind: Valentinstag, Squid Game, Ukraine/Russland-Krieg, Flüchtlingshilfe

Weitere Informationen

Proofpoint-Bericht zu Social Engineering herunterladen

Weitere Ressourcen

BLOG LESEN

Blog-Beitrag der Proofpoint-Bedrohungsforscher zu den seltsamsten Social-Engineering-Taktiken des letzten Jahres.

PODCAST ANHÖREN

Social Engineering: So manipulieren Bedrohungsakteure ihre Ziele. In diesem Podcast erklärt Proofpoint, wie Bedrohungsakteure unsere menschlichen Eigenschaften gegen uns ausnutzen.

KONTAKT

Vereinbaren Sie einen Termin mit Proofpoint, bei dem Sie erfahren, wie wir Ihr Unternehmen schützen können. Fordern Sie unsere kostenlose Risikobewertung an.

Weitere Informationen finden Sie unter proofpoint.com/de

MITARBEITER SCHÜTZEN. DATEN SICHERN.

Angreifer wissen, dass Ihre Mitarbeiter der einfachste Weg in Ihr Unternehmen sind. Schützen Sie Ihre Mitarbeiter mit zuverlässiger Sicherheit von Proofpoint. Jeden Tag schützen wir die Mitarbeiter bei mehr Fortune 500- und Global 2000-Unternehmen als alle anderen Sicherheitsanbieter.

Wir analysieren…

>2,6 Mrd. **E-Mail-Nachrichten**
>49 Mrd. **URLs**
>1,9 Mrd. **Anhänge**
> 28,2 Mio. **Cloud-Konten**
>1,7 Mrd. **Mobilgerätenachrichten**

…pro Tag

proofpoint.