Pressemitteilung

Cequence: Love Bots kursieren am Valentinstag

Dating-Apps waren 2023 Ziel von 660 Millionen Bot-Anfragen

München, 13. Februar 2024 – Cyberkriminelle sind rund um den Valentinstag (14. Februar) besonders aktiv auf Dating-Apps. Laut aktuellen Recherchen von Cequence Security versuchen sie, App-Nutzer zu manipulieren und ihnen finanziellen Schaden zuzufügen. Die Kriminellen geben sich dabei als echte Personen aus, bauen emotionale Bindungen auf, um nichtsahnenden App-Usern Geld zu entwenden. Das Threat Research Team des auf API-Sicherheit und Bot Management spezialisierten Lösungsanbieters Cequence analysierte weltweit anonymisierte Kundendaten zu Traffic und Angriffen auf Dating-Apps.

Die Ergebnisse im Überblick:

- 58 Prozent der Bot-Aktivitäten gehen im Jahr 2023 auf die USA zurück. Das ist ein Plus von 48 Prozent gegenüber 2021.
- 28 Prozent der Transaktionen betrafen iPhone Apps.
- 2023 gab es mehr als 660 Millionen Bot-Anfragen auf beliebten Dating-Apps.
- Cequence schützte mehr als 12 Millionen Accounts vor Account-Takeover-Attacken.

Neben dem Account Takeover (ATO), bei dem sich Kriminelle mit ausgefeilten Social-Engineering-Techniken Zugang zu Passwörtern verschaffen und dann Gelder transferieren, wird beim sogenannten „Romance Scam“ über Messages erst eine emotionale Beziehung aufgebaut. Anschließend erbitten die Betrüger den Kauf Dingen wie Blumen, Flugtickets oder gemeinsamen Reisen.

KI-Techniken steigern Erfolgsquote bei Betrügern

„Am Valentinstag nutzen Betrüger einsame Herzen auf Dating-Apps aus und suchen nach Möglichkeiten, Gelder zu erpressen“, sagt William Glazier, Director of Threat Research bei Cequence. „Kriminelle setzen mit den neuen Möglichkeiten von KI mehr und mehr auf Automatisierung, um ihre Operationen zu skalieren. Sie nutzen verstärkt APIs, um sich Zugang zu Nutzerkonten zu verschaffen. Betreiber und Entwickler von Dating- und Social-Apps müssen entsprechende Sicherheitsmaßnahmen ergreifen.“ Bots dienen Betrügern als Dreh- und Angelpunkt. Sie können damit ihre Angriffe skalieren.

„Betreiber von Dating-Seiten und -Apps brauchen eine langfristige, sichere Lösung gegen automatisierte Angriffe“, so Glazier weiter. „Im Rahmen einer ganzheitlichen Sicherheitsstrategie sind APIs in jeder Lebenszyklusphase zu schützen. API-Sicherheit und Bot Management sind dabei zusammen zu betrachten und nicht als

zwei verschiedene Aufgaben, die von unterschiedlichen Teams gelöst werden. Vielmehr geht es darum, alle APIs zu identifizieren und zu registrieren sowie die strikte Einhaltung von Industriestandards und den Einsatz moderner Tools sicherzustellen, um Bedrohungen zu erkennen und Angriffe abzuwehren."

Mehr Informationen auf www.cequence.ai

Pressekontakt:

Cequence Security
Mario van Riesen
Regional Sales Director DACH & CEE
Tel.: +49 151 7219 3673
Mail: mario@cequence.ai
Web: www.cequence.ai

VOCATO public relations GmbH
Birgit Brabeck
Friederike Wagner
Tel.: +49 2234 60198 - 18/-16
Mail: bbrabeck@vocato.com/fwagner@vocato.com
Web: www.vocato.com

Über Cequence Security

Cequence Security ist spezialisiert auf API-Sicherheit und Bot-Management. Mit seiner Unified-API-Protection-Plattform bietet es als einziges Unternehmen weltweit eine Lösung, die API-Erkennung, Compliance und Schutz für alle internen und externen APIs kombiniert, um Angriffe, gezielten Missbrauch und Betrug zu verhindern. Das flexible Bereitstellungsmodell benötigt weniger als 15 Minuten, um eine API ohne Programmierung, SDK oder JavaScript-Integration zu implementieren, und unterstützt SaaS-, Vor-Ort- und Hybrid-Installationen. Die Lösungen von Cequence sind so skalierbar, dass sie sich auch für anspruchsvolle Fortune- und Global-2000-Unternehmen eignen. Bei diesen Kunden sichern sie täglich mehr als 8 Milliarden API-Aufrufe und schützen mehr als 3 Milliarden Benutzerkonten. Weitere Informationen finden Sie unter www.cequence.ai

Bildmaterial:

Bild: William Glazier, Director of Threat Research bei Cequence Security.
Bildquelle: Cequence Security