

## Pressemitteilung

### **Cequence Security: Cyber-Betrug im Einzelhandel steigt um knapp 700 Prozent**

#### **Cyberkriminelle nutzen verstärkt Weihnachtsgeschäft aus**

**München, 14. Dezember 2023** – Allein in der zweiten Jahreshälfte 2023 stieg der Geschenkkartenbetrug im Einzelhandel um 110 Prozent, während unerwünschtes Scraping, Kunden- und Zahlungskartenbetrug durchschnittlich um mehr als 700 Prozent zunahmen. Das geht aus dem „[API Security Report](#)“ von [Cequence Security](#) zur Weihnachtssaison 2023 hervor. Für die Erhebung untersuchte der führende Unified-API-Protection-Lösungsanbieter Cequence Security die Verkehrs- und Angriffsdaten seiner Fortune-500- und Global-2000-Kunden, sowie Stichproben aus Milliarden von Transaktionen aus der Vor-Weihnachtssaison. Im Fokus standen dabei Retail-Kunden von Cequence.

#### **Differenzierte Angriffstaktik: Cyberangriffe über einen größeren Zeitraum verteilt**

Über den gesamten Kundenstamm hinweg identifizierte Cequence zwischen Juni und November 2023 automatisierte Cyberangriffe von 719 Millionen eindeutigen IP-Adressen und 325 Millionen bösartige Anmeldeversuche.

Der API Security Report zeigt, dass Cyberkriminelle ihre Taktik weiterentwickeln und sich für einen differenzierten Ansatz entscheiden. Das heißt, Angriffe werden über einen größeren Zeitraum verteilt und mit dem rechtmäßigen Datenverkehr vermischt, um so in der Haupteinkaufszeit der Weihnachtssaison nicht entdeckt zu werden.

„Die Weihnachtssaison 2023 hat eine erschreckende Realität offenbart: Cyberkriminelle setzen immer raffiniertere Angriffsmethoden ein und planen ihre Aktivitäten akribisch bereits Monate im Voraus, um Schwachstellen auszunutzen“, sagt William Glazier, Director Threat Research bei Cequence. Und weiter: „Dieser langfristige Ansatz ermöglicht es ihnen, unvorbereitete Einzelhändler und ahnungslose Kunden ins Visier zu nehmen, insbesondere während der Hochsaison. Das zeigt eindrucklich, wie wichtig es ist, das ganze Jahr über wachsam zu sein und proaktive Sicherheitsmaßnahmen zu ergreifen.“

#### **Kontoübernahmen und mit Produkten überschwemmte Warenkörbe**

Laut API Security Report stiegen Kontoübernahmen (Account Takeover, ATO) in der zweiten Hälfte des untersuchten Zeitraums für Einzelhändler um das 410-Fache. Cyberkriminelle hacken hierbei Online-Konten und verschaffen sich Zugriff auf Kunden-, Zahlungs- und weitere sensible Daten.

Darüber hinaus verzeichnet Cequence einen Anstieg von Shopping-Bots: Bei dieser Betrugsmasche wird eine hohe Anzahl von Produkten über Tools automatisiert zu Warenkörben hinzugefügt, um die Systeme zu überschwemmen und auf diese Weise so

viele gefragte Artikel wie möglich zu kaufen. Die Folge: Cyberkriminelle beherrschen den Markt und verhindern Verkäufe an legitime Kunden.

### **APIs ganzheitlich schützen**

Insgesamt zeigt die Analyse, wie dynamisch sich das API-Bedrohungsumfeld entwickelt und wie gerissen die Angreifer vorgehen. Mario van Riesen, Regional Sales Director DACH & CEE bei Cequence: „Um diese ausgefeilten Bedrohungen zu bekämpfen, die auf APIs abzielen, müssen Unternehmen ihre Abwehr mehr denn je mit einem ganzheitlichen Sicherheitsansatz verstärken. Ziel ist es, die APIs während ihres gesamten Lebenszyklus zu schützen.“

Mit der Unified-API-Protection-Plattform bietet Cequence Security eine umfassende End-to-End-Lösung für den gesamten API-Protection-Lebenszyklus – vom Aufdecken über das Monitoren bis hin zum Schutz aller im Unternehmen vorhandenen Schnittstellen.

Der vollständige Report ist als Download verfügbar: [„API Security Report“](#)

Mehr Informationen auf [www.cequence.ai](http://www.cequence.ai)

#### **Pressekontakt:**

Cequence Security  
Mario van Riesen  
Regional Sales Director DACH & CEE  
Tel.: +49 151 7219 3673  
Mail: [mario@cequence.ai](mailto:mario@cequence.ai)  
Web: [www.cequence.ai](http://www.cequence.ai)

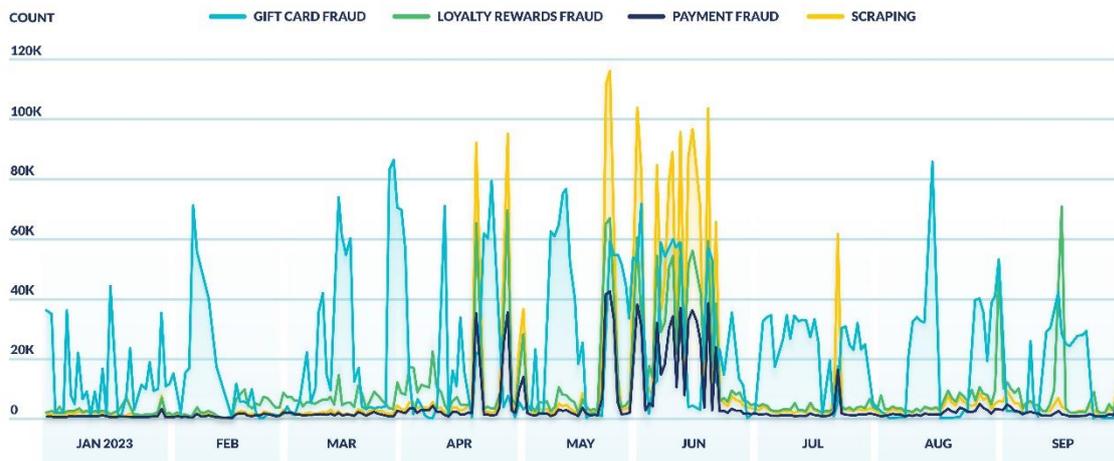
VOCATO public relations GmbH  
Birgit Brabeck /  
Friederike Wagner  
Tel.: +49 2234 60198 - 18 / - 16  
Mail: [bbrabeck@vocato.com](mailto:bbrabeck@vocato.com) / [fwagner@vocato.com](mailto:fwagner@vocato.com)  
Web: [www.vocato.com](http://www.vocato.com)

#### **Über Cequence Security**

Cequence Security bietet innovative Anwendungssicherheitslösungen für moderne hypervernetzte Unternehmen an. Das US-amerikanische Unternehmen mit Hauptsitz in Sunnyvale, Kalifornien, hat die Unified-API-Protection-Plattform entwickelt, die API-Erkennung, Inventarisierung, Compliance und dynamisches API Security Testing zur Echtzeit-Erkennung von Bedrohungen gegen sich ständig weiterentwickelnde Online-Angriffe in einer Lösung vereint. Hyperverbundene Unternehmen schützen damit ihre web-, mobil- und API-basierten Anwendungen vor Betrug, Geschäftsmissbrauch und Datenverlust. Gegründet 2014, sichert Cequence Security heute mehr als sechs Milliarden API-Transaktionen pro Tag und schützt mehr als zwei Milliarden Benutzerkonten der Fortune-500-Kunden. Weitere Informationen auf [www.cequence.ai](http://www.cequence.ai)

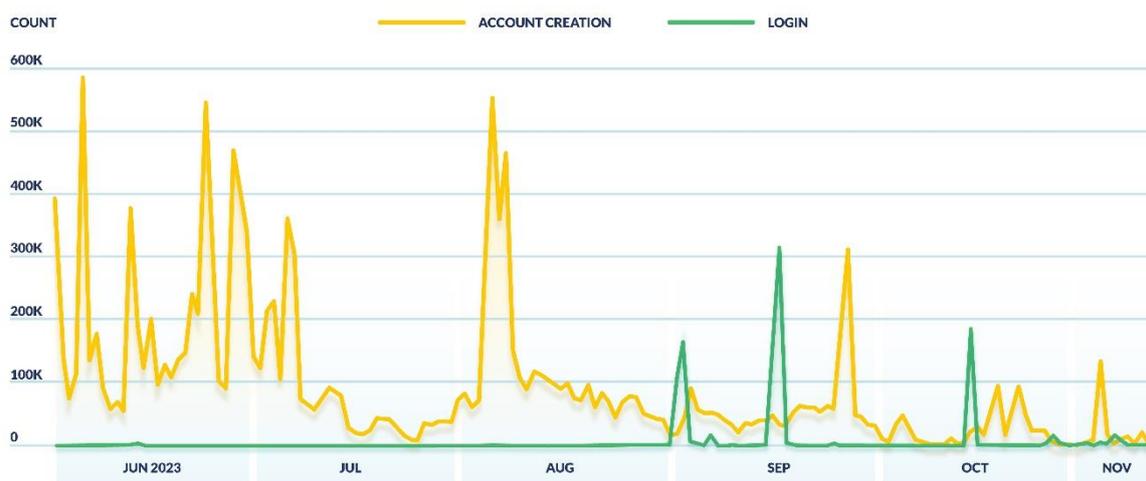
**Bildmaterial:**

**Types of Fraud Attempts Change Depending on Time of Year**



**Bild 1:** Laut „API Security Report“ von Cequence zur Weihnachtssaison 2023 stieg der Geschenkkartenbetrug im Einzelhandel allein in der zweiten Jahreshälfte 2023 um 110 Prozent, während unerwünschtes Scraping, Kunden- und Zahlungskartenbetrug durchschnittlich um mehr als 700 Prozent zunahmen. Dabei variieren die verschiedenen Arten von Betrugsversuchen je nach Jahreszeit. Einzelhändler sind mit ausgefeilten Angriffen von Cyberkriminellen konfrontiert, die unterschiedliche Taktiken, Techniken und Verfahren anwenden.

**Types of Fraud Attempts Are Concentrated at Different Times of the Year**



**Bild 2:** Betrügerische Aktivitäten werden bereits über Monate im Voraus vorbereitet und über einen größeren Zeitraum verteilt, um sich unentdeckt mit dem rechtmäßigen Datenverkehr zu vermischen. Während die betrügerische Kontoerstellung im erfassten Zeitrahmen abnahm, stiegen laut API Security Report die Kontoübernahmen (Account Takeover, ATO) in der zweiten Hälfte des untersuchten Zeitraums um das 410-Fache.



**Bild 3:** William Glazier, Director Threat Research, Cequence Security.



**Bild 4:** Mario van Riesen, Regional Sales Director DACH & CEE, Cequence Security.

*Bildquelle für alle Bilder: Cequence Security*