Lookout App Defense

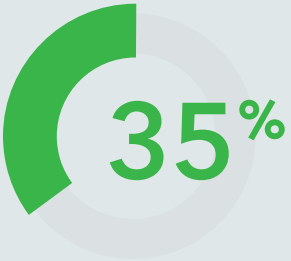
Proaktiv Risiken reduzieren und in Apps gespeicherte Kundendaten schützen

Apps – das neue Einfallstor für Cyberkriminelle

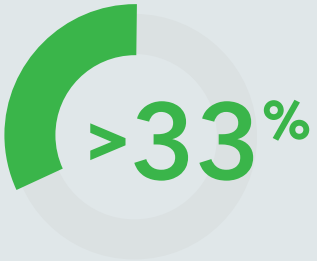
Smartphone-Apps sind mittlerweile ein unverzichtbarer Bestandteil unseres täglichen Lebens. Wir nutzen sie für alle möglichen Zwecke – von der Urlaubsbuchung bis zur privaten Finanzverwaltung. Dementsprechend setzen Unternehmen auf Apps, um ihren Kunden innovative Erlebnisse zu bieten und ihre Marken zu stärken. Doch die zunehmende Nutzung von Apps geht mit einer verschärften Cyber-Bedrohungslage einher. Böswillige Angreifer zielen nun vorwiegend auf Mobilgeräte ab, um Zugangs- und andere Kundendaten zu stehlen und sich so finanzielle Vorteile zu verschaffen oder zu Betrugszwecken falsche Identitäten zuzulegen. Einer der wichtigsten Bedrohungsvektoren, den sich Angreifer auf Mobilgeräten zunutze machen, sind die Apps selbst.

11.500

Zunahme der Anzahl an Malware-Paketen für Banking-Apps zwischen dem 4. Quartal 2018 und dem 1. Quartal 2019[1]



Weltweiter Zuwachs an In-App-Downloads zwischen 2016 und 2018[2]



aller betrügerischen Banking-Transaktionen erfolgen heute auf Mobilgeräten[3]

[1] Kaspersky Labs: „Phantom Menace: Mobile Banking Trojan Modifications Reach All-Time High“, 2018, www.kaspersky.com/about/press-releases/2018_phantom-menace.

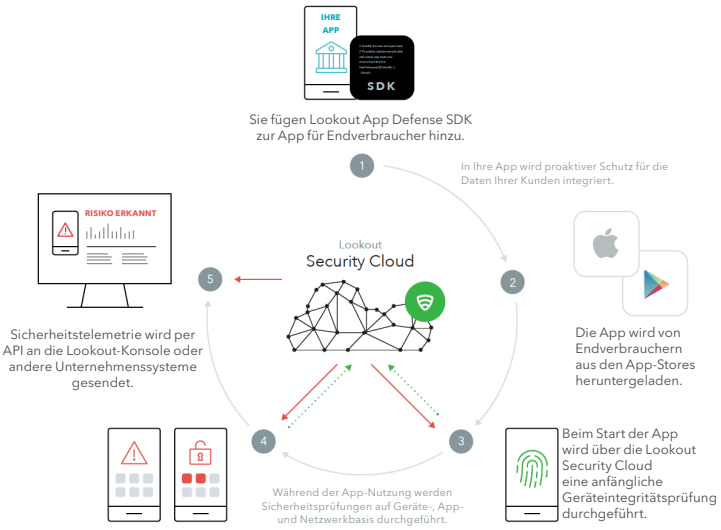
[1] App Annie: „The State of Mobile 2019: Banking and Finance“, 2019, www.appannie.com/en/go/state-of-mobile-2019/.

[1] RSA: „RSA Quarterly Fraud Report“, 2019, www.rsa.com/de-de/products/fraud-prevention/fraud-prevention.

Lookout App Defense SDK

Die Lookout App Defense-Lösung schützt Mobilgeräte-Apps über ein schlankes, integrierbares SDK für Android- und iOS-Geräte. Mit diesem integriertem SDK kann die App von der Lookout Security Cloud profitieren: Dort stehen Daten zu über 180 Millionen Geräten und 95 Millionen Apps bereit, um Privatpersonen und Organisationen vor Datenmanipulation durch Cyberbedrohungen und Malware zu schützen.

Unternehmen können die von Lookout App Defense erstellte Sicherheitstelemetrie abrufen und – je nach Art und Schweregrad der Bedrohung – mithilfe des SDK Risiken unterschiedlich bekämpfen. Zur Integration in vorhandene Sicherheitstools wie SIEM und Risikobewertungsmodelle bietet die Lookout Event Feed API einen Rohdaten-Feed für die Sicherheitsereignistelemetrie. Ganz allgemein kann das SDK dazu beitragen, Betrugs- und Datenmanipulationsrisiken zu mindern und gesetzliche Bestimmungen wie die DSGVO und die Zahlungsdiensterichtlinie zu erfüllen. Durch die Anzeige potenzieller Probleme während der App-Nutzung direkt auf dem Gerät werden zudem arglose Anwender geschützt.



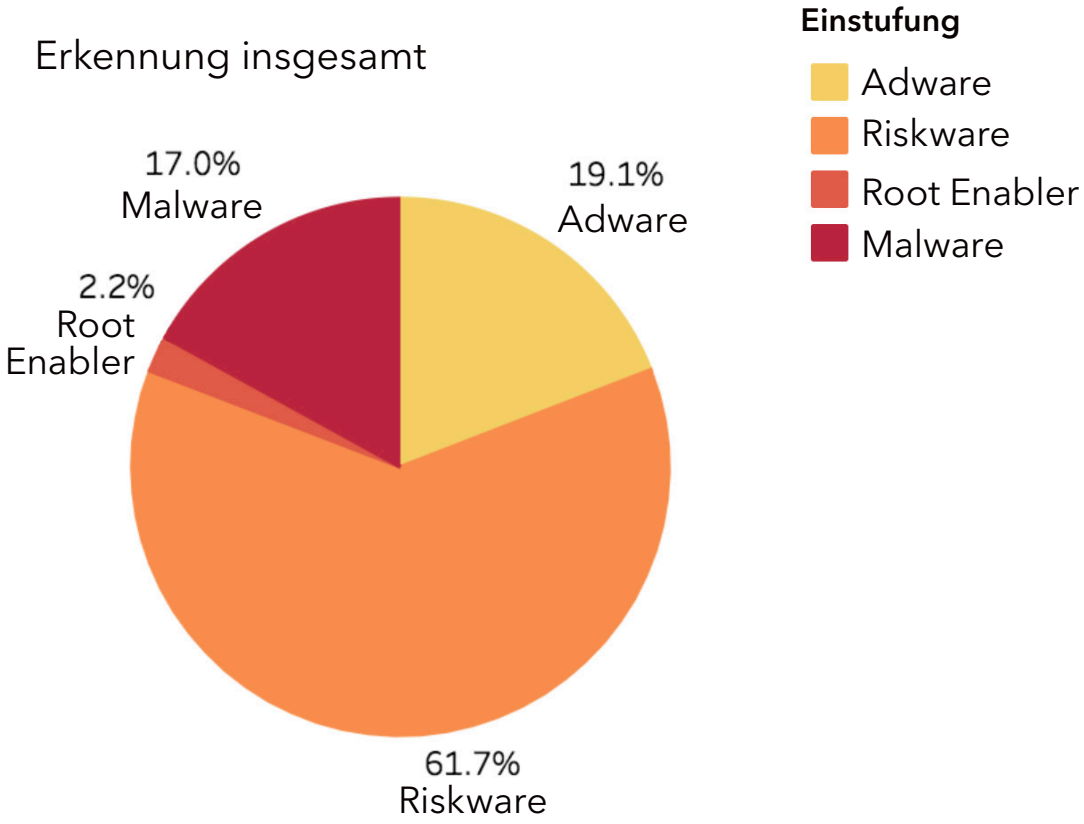
In-App-Schutz zur Erkennung und Beseitigung

Das SDK wirkt, indem es Mobilgeräte-Apps über diverse Workflows für Beseitigungsmaßnahmen mit Selbstschutzmechanismen sichert, ohne dabei das Anwendererlebnis zu stören oder zu beeinträchtigen. Nachstehend haben wir einige Beispiele für mögliche Erkennungs- und Beseitigungsschritte aufgeführt, die die App nach einer Warnung durch Lookout App Defense ergreifen könnte:

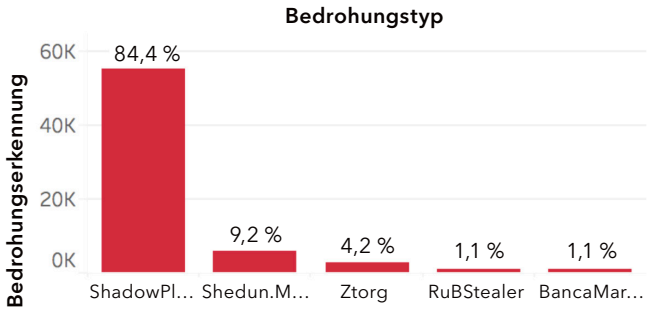
Erkennung (Schweregrad)	Beseitigung
Jailbreaking/Rooting und Rechteausweitung (hoch)	Authentifizierung blockieren oder Sitzung beenden
Zero-Day-Exploits und Man-in-the-Middle-Angriffe (hoch)	Sitzung beenden und Cache leeren
Root Enabler, Trojaner usw. (mittel)	Transaktionsumfang beschränken oder MFA aktivieren
Adware, Spyware und ähnliche Malware (niedrig)	Keine sofortige Beseitigung – Überwachung der Bedrohungen

Lookout App Risk Posture

Lookout App Risk Posture sorgt für maximale Transparenz, indem es für sämtliche Anwendergeräte, die die App eines Unternehmens verwenden, die Bedrohungsvektoren aufschlüsselt. Dazu gehört der Ausfall von Geräten, deren Betriebssystem nicht auf dem aktuellen Stand ist, die Rooting oder Jailbreaking zum Opfer gefallen sind oder die mit Malware infiziert wurden. Dazu wird jeweils eine Einstufung der Malware-Familie nach dem Schweregrad der Bedrohung angezeigt. Die folgenden Grafiken zeigen wichtige Daten aus der SDK-Telemetrie und der Lookout Security Cloud, anhand derer Sicherheits-, Betrugsbekämpfungs- oder Mobilgeräte-Teams ihre Risikomodelle optimieren und die Abwehr von Cyberbedrohungen verbessern können.



Trojaner – Top 5



Malware-Erkennung