Lookout Mobile Threat Landscape Report — 2023 Rückblick

Dieses Dokument ist eine Kurzfassung des Lookout Mobile Threat Landscape Report - 2023 Rückblick. Lesen Sie den vollständigen Bericht, um mehr Rückblicke und Trends im Bereich mobiler Schwachstellen, Mobile App Threats und OS basierten Risiken zu entdecken.

Zusammenfassung

Unabhängig davon, wie groß Ihr Unternehmen ist oder in welchem Sektor Sie tätig sind, 2023 erwies sich als ein evolutionäres Jahr für mobile Bedrohungen. Es gab eine Rekordzahl von Zero-Day-Schwachstellen in iOS, mehrere Entdeckungen beliebter Apps wie TikTok und PinDuoDuo mit riskanten Datenerfassungspraktiken, und die Cybercrime-Gruppe Scattered Spider bewies, dass mobiles Phishing ein äußerst effektiver Weg ist, um einige der weltweit größten Organisationen lahmzulegen.

Die Art und Weise, wie Bedrohungsakteure Unternehmen ins Visier nehmen und angreifen, verändert sich. Die Trends und Daten in diesem Jahresbericht zeigen, dass Angreifer verstärkt auf Social Engineering setzen und neue Angriffspunkte und Schwachstellen sowohl in der Software als auch bei den Mitarbeitern selbst ausnutzen. Aus diesem Grund gab es eine Rekordzahl von Phishing-Versuchen über mobile Geräte, die auf Unternehmensanwender abzielten. Darüber hinaus konnten bekannte Schwachstellen in mobilen Apps im Jahr 2023 ausgenutzt werden, indem die Zielperson per SMS, iMessage oder einer anderen mobilen App mit Messaging-Funktionalität auf eine schädliche Webseite geleitet wurde.

Dank der weltweit vielen Unternehmen, Behörden und Privatpersonen, die bei der Sicherung ihrer Endgeräte und Daten auf Lookout vertrauen, können wir auf basis unseres branchenführenden Datensatzes Millionen von Apps, Geräte und Web-Elemente analysieren. So sind wir in der Lage, globale Trends in der mobilen Bedrohungslandschaft frühzeitig zu erkennen.

Unternehmen jeder Größe und jeder Branche sind zunehmend stärker gefährdet, da mobile Geräte meist die am wenigsten geschützten Endpunkte sind. Dieser Bericht beweist, dass Cyberkriminelle ihre Taktik weiterentwickeln und mehrere Angriffsvektoren nutzen, die auf mobile Geräte abzielen, was bedeutet, dass IT-Teams neue Ansätze zum Schutz mobiler Geräte verfolgen müssen.

Phishing und bösartige Webinhalte

Mobiles Phishing ist heute eine der größten Herausforderungen für IT- und Sicherheitsteams. In der modernen Killchain ist diese Taktik die wohl effektivste Methode für Bedrohungsakteure, um Anmeldedaten von Mitarbeitern zu stehlen. Mit der zunehmenden Umgehung von MFA können sich Bedrohungsakteure in die Unternehmensinfrastruktur einloggen, um Informationen zu sammeln, Zugangsdaten zu erlangen und Daten zu kompromittieren.

Als eine der am häufigsten eingesetzten Lösungen zur Abwehr mobiler Bedrohungen bietet Lookout seinen Kunden einen sofort betriebsbereiten Schutz vor Phishing und bösartigen Inhalten sowie die Möglichkeit, benutzerdefinierte Inhaltsregeln und Blacklists zu erstellen.

431.000.000

Phishing- und bösartige Websites wurden von Lookout Security Cloud weltweit seit 2019 identifiziert.

54.000.000

Seiten mit verbotenen und anstößigen Inhalten wurden im Jahr 2023 gesperrt.

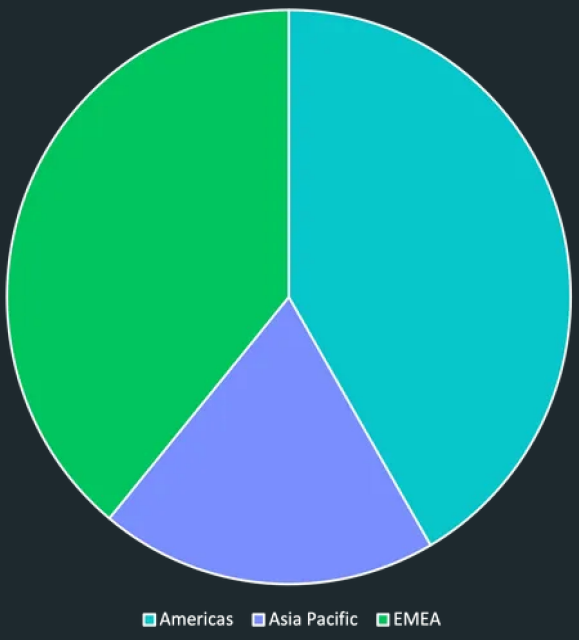
+

4.000.000

Angriffe durch Phishing und bösartige Internet-Attacken wurden 2023 durch Lookout verhindert.

58.000.000

Websites wurden von Lookout 2023 blockiert.



Lookout erkennt Entwicklungen auf jedem Kontinent, so dass Unternehmen, die in einer Vielzahl von Regionen tätig sind, die Behebung von Problemen in Regionen mit einer steigenden Anzahl von Angriffen priorisieren können.

Erfahren Sie außerdem mehr zu Rückblicken und Trends im Bereich mobiler Schwachstellen, Mobile App Threats und OS basierten Risiken. Jetzt den vollständigen Bericht lesen.

PRO TIP

Die Features, Funktionalitäten und Bildschirmgröße mobiler Geräte erschweren es dem Benutzer, Phishing-Angriffe zu erkennen. Lookout empfiehlt, bei SMS-Nachrichten von unbekannten Nummern, die ein Gefühl der Dringlichkeit vermitteln, nicht darauf einzugehen. Wenn die Nachricht angeblich von Ihrem IT-Team oder Ihrer Bank kommt, rufen Sie direkt dort an, um sich zu vergewissern, dass die Nachricht wirklich von dort gesendet wurde.

Über Lookout

Lookout, Inc. bietet datenzentrierte Cloud-Sicherheit, die verschiedene Phasen eines modernen Cybersecurity-Angriffs bewältigt. Daten sind das Herzstück eines jeden Unternehmens, und unsere Sicherheitsstrategie ist so konzipiert, das Daten in der sich ständig weiterentwickelnden Bedrohungslandschaft geschützt werden. Die Lookout Cloud Security Platform orientiert sich am Verhalten von Menschen, hilft, Bedrohungen in Echtzeit zu erkennen und Angriffe von den ersten Phishing-Versuchen bis zur Datenexfiltration schnell zu stoppen. Um mehr zu erfahren, besuchen Sie de.lookout.com, folgen Sie Lookout auf unserem Blog, LinkedIn und X.

Weitere Informationen finden Sie unter **de.lookout.com**

Holen Sie sich Ihre Demo-Version unter **de.lookout.com/contact/request-a-demo**

Lookout®