Betrüger nutzen den ChatGPT-Hype und verdienen mit Fleeceware-Apps Tausende von Dollar

Außer Spesen nichts gewesen: Sophos-Report deckt Abzocke durch kostspielige ChatGPT-Nachahmungen auf. Die Betrugs-Apps florieren weiterhin aufgrund von Lücken in den App-Store-Richtlinien und profitieren mit teils horrenden Abo-Gebühren vom aktuellen Interesse rund um die neueste Version des KI-gestützten Sprachmodells.

Sophos X-Ops hat verschiedene Apps in den offiziellen Stores von Apple und Google aufgedeckt, die sich als legitime, ChatGPT-basierte Chatbots ausgeben, Nutzer mit verschleierten, oftmals enorm hohen Gebühren abzocken und den Betrügern so monatlich Tausende von Dollar in die Tasche spülen. Der Report „FleeceGPT Mobile Apps Target AI-Curious to Rake in Cash" deckt die Machenschaften dieser sogenannten „Fleeceware"-Programme auf, bei der Nutzer mit nahezu null Funktionalität sowie ständigen Werbeeinblendungen in kostenlosen Testvarianten zu einem kostenpflichtigen Abo getrieben werden sollen. Zudem steigern die Betrüger die Attraktivität ihre Apps durch gefälschte Bewertungen und ständige Aufforderungen der Nutzer, die App zu bewerten, bevor sie überhaupt verwendet wird oder die kostenlose Testversion endet.

„Betrüger haben und werden immer die neuesten Trends oder Technologien nutzen, um ihre Taschen zu füllen. ChatGPT ist da keine Ausnahme. Da das Interesse an KI und Chatbots zurzeit extrem groß ist, laden Benutzer aktuell nahezu alles sehr unreflektiert herunter, das ChatGPT ähnelt – ein Verhalten, dass den Entwicklern dieser Art von Betrugs-Apps, Sophos nennt sie „Fleeceware", natürlich in die Karten spielt. Sie gehen davon aus, dass die Nutzer nicht auf die Kosten achten oder einfach vergessen, dass sie ein Abonnement abgeschlossen haben. Die Fleeceware-Apps sind speziell so konzipiert, dass sie nach Ablauf der kostenlosen Testversion kaum noch oder gar nicht mehr genutzt werden können. Das ist besonders heimtückisch, da selbst beim Löschen der App die Abozahlungen oftmals weiterlaufen. Nutzer, die auf Fleeceware-Apps hereingefallen sind, sollten deshalb auf jeden Fall die Richtlinien der App-Stores von Apple und Google zum offiziellen Abmelden befolgen," so Sean Gallagher, Principal Threat Researcher bei Sophos.

Das Original ist in der Grundversion kostenlos, die Fakes hingegen bitten sofort zur Kasse

Im aktuellen Report untersuchte Sophos X-Ops fünf Fleeceware-Apps, die alle angeblich auf dem ChatGPT-Algorithmus basieren, näher. In einigen Fällen, wie bei der App „Chat GBT", nutzen die Entwickler die Namensähnlichkeit zum Original aus, um das Ranking ihrer App im Google Play oder App Store zu verbessern. Während OpenAI allerdings den Nutzern die Grundfunktionalität von ChatGPT kostenlos zur Verfügung stellt, kosten diese Apps zwischen 10 US-Dollar pro Monat und 70,00 US-Dollar pro Jahr – und das ohne jeglichen Mehrwert. Die iOS-Version von „Chat GBT", genannt „Ask AI Assistant", kostet nach der dreitägigen, kostenlosen Testversion 6 US-Dollar pro Woche – oder 312 US-Dollar pro Jahr – und spülte den Machern allein im März über 10.000 US-Dollar in die Kassen; trotz zahlreicher negativer Bewertungen. Die genaue Analyse

dieser und aller anderen betrügerischen Apps kann im Report „FleeceGPT Mobile Apps Target AI-Curious to Rake in Cash" nachgelesen werden.

„Fleeceware-Apps sind speziell darauf ausgelegt, in puncto Service am Rande der von Google und Apple erlaubten Möglichkeiten zu bleiben, und sie verstoßen nicht gegen die Sicherheits- oder Datenschutzbestimmungen, sodass sie von diesen Stores bei der Überprüfung nur sehr selten abgelehnt werden", so Gallagher. „Während Google und Apple neue Richtlinien zur Eindämmung von Fleeceware eingeführt haben, seit wir 2019 über solche Apps berichtet haben, finden Entwickler immer wieder Möglichkeiten, diese Richtlinien zu umgehen, indem sie beispielsweise die Nutzung und Funktionalität von Apps stark einschränken, sofern die Benutzer nicht zahlen. Trotz der Löschung einiger aktueller Betrugs-Apps ist davon auszugehen, dass immer wieder neue auftauchen. Der beste Schutz ist deshalb Aufklärung. Benutzer müssen sich darüber im Klaren sein, dass diese Art von betrügerischen Apps existiert und immer das Kleingedruckte lesen, bevor sie auf Abonnieren klicken. Zudem sollten Benutzer Apps an Apple und Google melden, wenn sie der Meinung sind, dass die Entwickler unethische Mittel einsetzen, um Profit zu machen."

Alle im Bericht erwähnten Apps wurden gemeldet, Google hat einen Teil der Apps auf seiner Plattform zum Zeitpunkt des Blogbeitrags gelöscht, Apple hat den Eingang der Information bestätigt. Benutzer, die diese Apps bereits heruntergeladen haben, sollten die Richtlinien des Apple-App- oder Google-Play-Stores zum „Abmelden" befolgen. Durch einfaches Löschen der Fleeceware-App erlischt das Abonnement nicht immer automatisch.

Hier gibt es nähere Infos zum betrügerischen Einsatz von Fleeceware auf Google Play und im Apple App Store.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de