Betrügerische „CryptoRom“-Apps schleichen sich in App-Stores von Apple und Google

Cyberkriminelle unterwandern die Sicherheits-Checks von App-Store-Betreibern mithilfe von sich ändernden Remote-Inhalten. Anschließend gelistet im offiziellen Apple App Store und Google Play Store ist den Cyberkriminellen Tür und Tor für ihre Betrügereien geöffnet.

Sophos veröffentlicht heute in seinem Bericht „Fraudulent Trading Apps Sneak into Apple and Google App Stores“ neue Erkenntnisse über die CryptoRom-Betrugsmasche, auch als „Pig Butchering“-Methode bekannt. Hierbei handelt es sich um professionelle Finanzbetrüger, die Nutzer von Dating-Apps ködern und im Verlauf einer vorgetäuschten Liebesbeziehung dazu verleiten, vermeintliche Investitionen in Kryptowährungen zu tätigen. Tatsächlich fließen die Gelder aber direkt in die Taschen der Betrüger. Während Cyberkriminelle bislang Workaround-Techniken nutzten, um Opfer davon zu überzeugen, illegitime iPhone-Apps herunterzuladen, die nicht vom Apple App Store geprüft und zertifiziert wurden, haben sie es nun erstmals geschafft, gefälschte CryptoRom-Apps direkt in den offiziellen App Store zu platzieren. Im Google Play Store sind bereits vorher Apps diese Art gesichtet worden.

Die Apps „Ace Pro“ und „MBM_BitScan“ haben die strengen Sicherheitsprotokolle von Apple erfolgreich umgangen und sind damit einer riesigen Zielgruppe zugänglich gewesen. Sophos benachrichtigte Apple sofort über seinen Fund und die betrügerischen Apps wurden aus dem App Store entfernt. Die App MBM-BitScan war zudem im Play Store unter dem Namen BitScan zu finden. Auch Google wurde von Sophos umgehend über die App informiert und hat diese aus dem Store entfernt.

„Während wir Fake-Apps im Play Store bereits aus der Vergangenheit kennen, ist es nun das erste Mal, dass wir solche Anwendungen im Apple App Store gefunden haben. Im Allgemeinen ist es schwierig, Malware durch den Sicherheitsüberprüfungsprozess im Apple App Store zu bringen“, so Jagadeesh Chandraiah, Senior Threat Researcher bei Sophos. „Aus diesem Grund mussten Betrüger, die auf iOS-Geräte abzielten, die Anwender davon überzeugen, zuerst ein Konfigurationsprofil zu installieren, bevor sie die gefälschte Handels-App installieren konnten. Dies beinhaltet eine zusätzliche Ebene des Social Engineering – eine Ebene, die schwer zu überwinden ist. Viele potenzielle Opfer werden stutzig, dass etwas nicht stimmt, wenn sie eine vermeintlich legitime App nicht direkt herunterladen können. Indem die Cyberkriminellen nun Anwendungen direkt in den Apple App Store bringen konnten, haben sie ihren potenziellen Opferpool enorm vergrößert und profitieren zudem von der Tatsache, dass die meisten Benutzer Apple von Natur aus vertrauen. Beide von uns gefundenen Apps haben zudem nicht den neuen Lockdown-Modus von iOS ausgelöst, der Betrüger daran hindert, mobile Profile zu laden, die für Social Engineering hilfreich sind. Angesichts der Sicherheitsfunktionen in Lockdown ändern die die Betrüger möglicherweise ihre Taktik – d. h. sie konzentrieren sich darauf, den Überprüfungsprozess im App Store zu umgehen.“

Den Betrügern verfallen

In einem konkreten Fall, bei dem das Opfer mit Ace Pro betrogen wurde, köderten die Betrüger das Ziel mit einem gut gefälschten Facebook-Profil einer Frau, die angeblich einen verschwenderischen Lebensstil in London führt. Nachdem sie eine Beziehung zum Opfer aufgebaut hatte, wechselten die Betrüger mit dem Opfer zu WhatsApp und überzeugten die Person dort davon, die betrügerische Ace Pro-App herunterzuladen. Von dort aus entfaltete sich der Kryptowährungsbetrug.

App als Fliegenfalle
Ace Pro wurde im App Store als QR-Code-Scanner beschrieben, ist aber eine betrügerische Krypto-Handelsplattform. Nach dem Öffnen sehen Benutzer eine Handelsplattform, auf der sie angeblich Währungen einzahlen und abheben können. Das eingezahlte Geld geht jedoch direkt an die Betrüger. Um die Sicherheit des App Store zu umgehen, gehen die Sophos-Forscher davon aus, dass die Betrüger die App mit einer Website mit harmlosen Funktionen verbunden haben, als sie ursprünglich zur Überprüfung eingereicht wurde. Die Domain enthielt Code für das QR-Scannen, damit sie für App-Kontrolleure legitim aussieht. Sobald die App jedoch genehmigt wurde, leiteten die Betrüger die App auf eine in Asien registrierte Domain um. Diese Domain sendet eine Anfrage, die mit Inhalten von einem anderen Host antwortet, der letztlich die gefälschte Handelsplattform liefert.

Die Apple App MBM_BitScan verfolgt einen ähnlichen Ansatz und treibt auch auf Android-Geräten ihr Unwesen, dort ist sie jedoch nur als „BitScan“ gelistet. Sowohl die App aus dem Apple App Store als auch aus Google Play kommunizieren mit derselben Command-and-Control-Infrastruktur, die dann wiederum mit einem Server Kontakt aufbaut, der einer legitimen japanischen Kryptofirma ähnelt. Diese Fake-Seiten werden in Runtime geladen, die bösartigen Inhalte verbleiben auf dem Web-Server und nicht im Anwendungscode. Die Aufdeckung ist so sehr schwierig, da es für die Tester eben nicht ausreicht, nur den Code zu betrachten.

Die einzelnen Schritte der CryptoRom-Betrüger und weitere Details zum Unterlaufen der App-Store-Sicherheitsprozesse gibt es im offiziellen, englischsprachigen Bericht „Trading Apps Sneak into Apple and Google App Stores“.

Was ist CryptoRom?
Bei CryptoRom handelt es sich um eine Cyber-Betrugsmasche, die auch als „Pig Butchering“ bekannt ist. Die Kriminellen setzten hierbei auf ein professionell organisierte, syndizierte Betrugsoperation, die eine Kombination aus romantischen Social Engineering und betrügerischen Krypto-Handelsanwendungen verwendet. Nachdem eine Vertrauensbasis aufgebaut wurde, werden die Opfer über gut gemachten Fake-Handelsplattformen um ihr Erspartes gebracht. Sophos X-Ops verfolgt und berichtet über diese Betrügereien bereits seit längerem und geht von einem Schaden in Millionenhöhe aus.

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
Ariane Wendt +49-172-4536839
sophos@tc-communications.de