Falsche Freunde, falsche Apps:
Sophos findet 167 gefälschte Handels- und Kryptowährungs-Apps

Über Dating-Websites oder täuschend echte gefälschte Banken-Websites wurden Nutzer angesprochen und dazu verleitet, als beliebte Marken getarnte Gauner-Apps zu installieren

Sophos hat 167 gefälschte Android- und iOS-Apps identifiziert, mit denen Nutzer, im guten Glauben eine seriöse Finanzhandels-, Bank- oder Kryptowährungs-App installiert zu haben, um ihr Geld gebracht wurden. Der Bericht "Fake Android and iOS apps disguised as trading and cryptocurrency apps," zeigt auf, wie die Opfer mithilfe von Social-Engineering-Techniken oder gefälschten Websites, darunter unter anderem auch ein falscher iOS-App-Store und eine iOS-App-Test-Website, dazu verleitet wurden, die schadhaften Apps herunter zu laden.
Die Betrugs-Apps fanden sich im asiatischen Raum, bei gutem Erfolg für die Betrüger könnte das Beispiel auch weltweit Schule machen.

Vermutlich eine Gruppe von Cyberbetrügern
Einige der Apps enthielten eine eingebettete "Chat"-Option für den Kundensupport. Beim Versuch, mit den Support-Teams über den Chat zu kommunizieren, erhielten die Sophos-Forscher sprachlich nahezu identische Antworten. Dies und die Tatsache, dass 167 Apps sich alle auf einem Server befanden, deutet laut Sophos darauf hin, dass die Betrügereien alle von derselben Gruppe betrieben werden könnten.

Doppelt getäuscht: Freundschaft fake, Geld futsch
Bei einem der untersuchten Betrugsversuche freundeten sich die Betrüger über eine Dating-App mit Benutzern an, richteten ein Profil ein und tauschten Nachrichten aus, bevor sie schließlich versuchten, ihre Chatpartner dazu zu verleiten, eine gefälschte App zu installieren und dort Geld und Kryptowährung hinzuzufügen. Versuchte das Opfer später, Geld abzuheben oder das Konto zu schließen, blockierten die Angreifer einfach den Zugang.
Eine andere Masche bestand darin, Opfer mit Websites zu ködern, die denen einer vertrauenswürdigen Marke wie einer Bank ähneln. Die Betrüger haben sogar eine gefälschte Download-Seite für den „iOS App Store" mit gefälschten Kundenbewertungen eingerichtet, um Nutzern vorzugaukeln, dass sie eine App aus dem Original-App-Store installieren. Wenn Personen auf die Links zum Herunterladen der gefälschten Apps für Android oder iOS klickten, erhielten sie etwas, das wie eine mobile Web-App aussah, aber in Wirklichkeit ein Shortcut-Symbol war, das zu einer gefälschten Website führte.
Einige der gefälschten iOS-Apps wurden auch über Websites von Drittanbietern verbreitet, bei denen iOS-Entwickler neue Anwendungen mit einer begrenzten Anzahl von Nutzern von Apple-Geräten testen können, bevor sie Apps für den offiziellen App Store einreichen.

Seriöse Quellen nutzen und wie immer: Augen auf bei Superangeboten
"Menschen vertrauen den Marken und Personen, die sie kennen oder glauben, zu kennen - und die Betreiber hinter diesen gefälschten Handels- und Kryptowährungs-Apps nutzen das rücksichtslos aus", sagt Michael Veit, Security Evangelist bei Sophos.
Sophos empfiehlt zum Schutz vor falschen Apps:

- Apps sollten nur aus vertrauenswürdigen Quellen wie Google Play und Apples App Store installieret werden. Die Entwickler beliebter Apps haben oft eine Website, die die Benutzer zur echten App leitet. Wenn möglich, sollten Benutzer überprüfen, ob die App, die sie installieren wollen, von ihrem tatsächlichen Entwickler erstellt wurde.
- Wie immer gilt auch hier: Wenn etwas riskant oder zu gut erscheint, um wahr zu sein, ist es das meist auch nicht. Vorsicht also bei Versprechen von verdächtig hohen

Investitionsrenditen oder Gesprächspartnern auf einer Dating-Website, die dazu auffordern, Geld oder Kryptowährungswerte auf ein 'tolles' Konto zu überweisen...
- Mobile Geräte sollten mit einer Antiviren-App geschützt werden, wie z.B. Intercept X for Mobile, um Android- und iOS-Geräte vor Cyber-Bedrohungen zu schützen.

Den gesamten Bericht finden Sie hier:
Fake Android and iOS apps disguised as trading and cryptocurrency apps

Neu: 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: http://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