**Fałszywe aplikacje do kryptowalut na iOS – nowe oszustwo celujące w użytkowników iPhone’ów**



**Kraków, 15 października 2021 –** Badacze Sophoswykryli nowy rodzaj oszustwa, którego ofiarami padają **użytkownicy systemów iOS** w USA i Europie. Cyberprzestępcy, wykorzystując fałszywe profile w serwisach randkowych takich jak Tinder, Grindr czy Facebook Dating, nakłaniają do zainstalowania **złośliwych aplikacji do handlu kryptowalutami**. Za ich pomocą nie tylko kradną środki finansowe, ale mogą też mieć **zdalny dostęp do iPhone’ów ofiar**. Na konto przestępców stosujących ten mechanizm wpłynęło już co najmniej **1,39 mln dolarów**.

**(Nie)bezpieczny App Store**

Cyberprzestępcy zakładają fałszywe profile na portalach randkowych (Tinder, Bumble, Facebook Dating i Grindr) i nawiązują kontakt z ofiarą. W kolejnym kroku nakłaniają ją do zainstalowania **fałszywej aplikacji Binance** **do handlu kryptowalutami**. Po zainwestowaniu w niej niewielkiej kwoty pozwalają użytkownikowi wypłacić pieniądze z zyskiem. Następnie zachęcają do wyłożenia większych środków. Kiedy ofiara nabiera podejrzeń lub chce odzyskać pieniądze, zostaje **zablokowana**. Przestępcy zarabiają na tym procederze **miliony dolarów** – badacze Sophos wyśledzili adres portfela bitcoin, na który oszukane osoby wysłały już **ponad 1,39 mln** dolarów. Prawdopodobnie takich adresów jest więcej.

**–** *Już na początku roku Interpol ostrzegał przed rosnącą skalą oszustw dokonywanych przez aplikacje randkowe i media społecznościowe. Teraz celem są głównie użytkownicy iPhone’ów. Chociaż platforma iOS jest ogólnie uważana za bezpieczną, nawet aplikacje w App Store mogą stanowić zagrożenie. Pełno jest tam na przykład „darmowych” programów typu fleeceware, które po kilku dniach obciążają użytkowników kilkutysięcznymi subskrypcjami.**Oszustwo wykorzystujące fałszywe aplikacje do kryptowalut omija kontrole bezpieczeństwa App Store. Użytkownicy systemu iOS powinni więc mieć się na baczności* **–** wskazuje **Grzegorz Nocoń, inżynier systemowy w firmie Sophos**.

**Kradzież pieniędzy i danych osobowych**

Cyberprzestępcy do rozpowszechniania fałszywych aplikacji wykorzystują **system dla programistów Enterprise Signature**, który umożliwia testowanie aplikacji na iOS zanim zostaną zatwierdzone przez Apple. Dzięki temu przestępcy mogą rozsyłać do użytkowników iPhone'ów fałszywe programy bez recenzji App Store. W ten sposób zyskują też **zdalny dostęp do urządzeń** ofiar. Potencjalnie mogą więc **zbierać dane osobowe**, dodawać lub usuwać konta, instalować aplikacje i zarządzać nimi.

Enterprise Signature był już wcześniej używany przez przestępców. Apple podjęło działania aby ukrócić proceder. Za rozsyłanie aplikacji do konsumentów tą drogą cofnięto nawet certyfikaty Google’a i Facebooka (potem zostały przywrócone). Nie uniemożliwiło to jednak omijania kontroli App Store.

**–** *Oszuści są nadal aktywni, każdego dnia kolejne ofiary mogą zostać nakłonione do zainwestowania pieniędzy, z niewielką szansą na ich odzyskanie. Apple powinien ostrzegać użytkowników instalujących aplikacje za pośrednictwem systemu Enterprise, że nie zostały one sprawdzone. Właściciele iPhone'ów powinni natomiast instalować wyłącznie programy z App Store. Kluczowa zasada, o której trzeba pamiętać brzmi: jeśli coś jest zbyt piękne, aby było prawdziwe, np. nowo poznana osoba wspomina o inwestycji, która zapewni duży zysk, to niestety zazwyczaj jest to oszustwo* – przestrzegai **Grzegorz Nocoń.**

**O firmie Sophos**

Sophos jest światowym liderem zabezpieczeń nowej generacji. Chroni przed najbardziej zaawansowanymi cyberzagrożeniami ponad 500 tys. firm i miliony konsumentów w ponad 150 krajach. Przy wsparciu AI, uczenia maszynowego i inteligentnej analizy zagrożeń zespołu SophosLabs i SophosAI, firma oferuje szerokie portfolio zaawansowanych produktów i usług. Pomagają one zabezpieczyć użytkowników, sieci i urządzenia końcowe przed zagrożeniami takimi jak ransomware, malware, exploity, phishing i inne. Platforma do zarządzania w chmurze Sophos Central integruje całe portfolio produktów nowej generacji Sophos w jeden system „zsynchronizowanej ochrony”. To adaptacyjny ekosystem cyberbezpieczeństwa, który wykorzystuje bogaty zestaw otwartych interfejsów API dostępnych dla klientów, partnerów, deweloperów i innych dostawców cyberbezpieczeństwa. Sophos sprzedaje swoje produkty i usługi za pośrednictwem globalnej sieci partnerów i dostawców usług zarządzanych (MSP). Firma ma siedzibę w Oksfordzie w Wielkiej Brytanii. Więcej informacji można znaleźć na stronie [www.sophos.com](http://www.sophos.com/).