INFORMACJA PRASOWA

Katowice, 26.10.2021 r.

Cyberprzestępcy coraz śmielej atakują posiadaczy kryptowalut. Na celowniku użytkownicy kryptowaluty SafeMoon

Cyberprzestępcy próbują wykorzystać kolejną wielką okazję, jaką jest system kryptowalut. Przejmując zdalną kontrolę nad komputerami nieświadomych użytkowników, starają się wykraść ich hasła oraz pieniądze. Badacze cyberbezpieczeństwa ESET dostrzegli niedawno nową kampanię podszywającą się pod aplikację kryptowalutową SafeMoon. – Wykorzystując fałszywą aktualizację do aplikacji atakujący wabią użytkowników komunikatora Discord na stronę internetową, która rozpowszechnia złośliwe oprogramowanie umożliwiające zdalny dostęp do komputerów ofiar – ostrzega ekspert ESET.

SafeMoon – kolejna kryptowaluta w obszarze zainteresowań cyberprzestępców

SafeMoon to jeden z najnowszych altcoinów, który powstał na fali pojawiania się alternatywnych dla popularnego Bitcoina kryptowalut i tokenów. Obecnie na całym świecie funkcjonuje już ponad 5 tysięcy różnych altcoinów. Od momentu powstania sześć miesięcy temu, SafeMoon cieszy się dużą popularnością. Zainteresowanie nią jest stale napędzane przez wpływowych i licznych entuzjastów w mediach społecznościowych. Wśród rekomendujących nową kryptowalutę znaleźli się m.in. amerykański youtuber Logan Paul i raper Lil Yachty. Szum wokół nowego rodzaju altcoina nie umknął również uwadze cyberprzestępcoów, którzy często wykorzystują do swoich oszustw popularne aplikacje lub tematy wspierane przez znane i wpływowe osoby. Nierzadko korzystają z nazwisk celebrytów, aby nadać swoim działaniom wiarygodności i atrakcyjności. W przypadku SafeMoon podstęp zaczyna się od wiadomości, którą oszuści wysyłają do użytkowników na komunikatorze Discord, w której podszywają się pod oficjalne konto aplikacji do kryptowalut, aby promować jej rzekomą aktualizację.

– Po kliknięciu w adres URL dołączony do wiadomości, użytkownik zostaje przeniesiony na spreparowaną stronę, która ma odzwierciedlać część oficjalnego serwisu SafeMoon, a dokładniej jego starszą wersję. To nie pierwszy raz, kiedy oszuści wykorzystują tego rodzaju sztuczki. Chociaż spreparowana witryna jest niemal identyczna, to spostrzegawczy użytkownicy mogą dostrzec różnicę w adresie strony, która zawiera dodatkową literę. Oczywiście cyberprzestępcy liczą, że większość nieświadomych użytkowników nie zauważy drobnej różnicy i w pośpiechu pobierze fałszywą aktualizację – mówi **Beniamin Szczepankiewicz**, starszy specjalista ds. cyberbezpieczeństwa ESET.

Adres korespondencyjny:
DAGMA Sp. z o.o. | ul. Pszczyńska 15 | Katowice (40-478)
tel. 32 793 11 00 | handel@dagma.pl
www.dagma.com.pl

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852

Fałszywa strona, prawdziwe linki – oszuści coraz lepiej przygotowani

Jak twierdzą badacze ESET wszystkie linki zewnętrzne na spreparowanej stronie były legalne, z wyjątkiem linku, który zachęca do pobrania rzekomej aktualizacji aplikacji SafeMoon w sklepie Google Play. Zamiast aplikacji do kryptowalut na urządzenia z systemem Android użytkownik pobiera złośliwy plik wraz z instalatorem. Po uruchomieniu aplikacja umieszcza w systemie użytkownika kilka plików, w tym złośliwe oprogramowanie o nazwie Remcos. Ten złośliwy program (typu RAT) może umożliwić atakującym w pełni zdalne zarządzanie systemem ofiary.

– Remcos pozwala atakującemu pozyskać wiele poufnych danych użytkownika. Możliwości Remcos obejmują m.in kradzież danych logowania z różnych przeglądarek internetowych, rejestrowanie wciskanych klawiszy, rejestrowanie obrazu z kamery internetowej, przechwytywanie dźwięku z mikrofonu ofiary oraz pobieranie i uruchamianie dodatkowego złośliwego oprogramowania na sprzęcie ofiary – ekspert ESET.

W jaki sposób skutecznie się chronić?

Rynek kryptowalut jest mocno wykorzystywany przez cyberprzestępców do oszustw. Jak niemal w każdej aktywności internetowej, również w przypadku kryptowalut, należy zwracać szczególną uwagę na otrzymywane wiadomości. Chociaż działania przestępców są coraz bardziej zaawansowane, to kilka podstawowych środków ostrożności pozwoli zabezpieczyć się przed kradzieżą danych i pieniędzy:

- Uważaj na wszelkie nieoczekiwane komunikaty, przesyłane za pośrednictwem poczty e-mail, mediów społecznościowych, SMS-ów lub innych kanałów komunikacyjnych
- Nie klikaj „z automatu” w linki w wiadomościach, a przed kliknięciem zawsze weryfikuj nadawcę – upewnij się, że jest zaufany
- Uważaj na nieprawidłowości w adresach URL (np. literówki) – ich obecność to sygnał ostrzegawczy
- Używaj silnych i unikalnych haseł oraz, jeśli to możliwe, uwierzytelniania dwuskładnikowego
- Korzystaj z kompleksowego oprogramowania zabezpieczającego, który może ostrzec przed spreparowanymi stronami internetowymi

Adres korespondencyjny:
DAGMA Sp. z o.o. | ul. Pszczyńska 15 | Katowice (40-478)
tel. 32 793 11 00 | handel@dagma.pl
www.dagma.com.pl

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852