**Hakerzy wykradli nagie zdjęcia amerykańskich celebrytek – czy zabezpieczenia iCloud zostały złamane?**

**Kilka dni temu świat obiegła informacja o wycieku setek prywatnych (często intymnych) zdjęć amerykańskich celebrytek. Czy zawiniła architektura bezpieczeństwa Apple’a? W jaki sposób hakerzy uzyskali dostęp do dawno usuniętych zdjęć jednej z gwiazd? Posiadając nazwę użytkownika i hasło hakerzy są w stanie odzyskać wcześniejsze kopie zapasowe ofiary – twierdzi Moit Sagey z firmy Check Point.**

Pod koniec sierpnia do Internetu, w wyniku ataku hakerskiego, wyciekły prywatne zdjęcia amerykańskich celebrytów, na co dzień posługujących się urządzeniami moblinymi z logiem jabłuszka. Wśród ofiar hakerów były między innymi: **Jennifer Lawrence**, **Kristen Dunst**, **Ariany Grande** czy **Kate Upton.** Po kilku dniach od incydentu, który wstrząsnął śmietanką towarzyską Hollywood, firma Apple, do usług której usług włamali się hakerzy, zdementowała informacje, jakoby doszło do naruszenia zabezpieczeń iCloud. W swoim oświadczeniu zaznaczyła, że po ponad 40-godzinnym śledztwie, doszła do wniosku,iż *niektóre konta celebrytów zostały naruszone przez namierzony i zaplanowany atak na nazwy użytkownika, hasła i pytania zabezpieczające(…) W żadnym z przebadanych przypadków, nie stwierdzono jakiegokolwiek systemu Apple’a, włączając iCloud czy Find my iPhone.*

Niezależni eksperci niekoniecznie podzielają stanowiska firmy z Cupertino. **Johnatan Zdziarski, informatyk śledczy**, na swoim profilu twitterowym stwierdził, że Apple mogło zrobić znacznie więcej w celu zabezpieczenia kont użytkowników, jak *niedopuszczenie do niekończących się prób ataków, przez weryfikację* *logowań z nieznanych adresów IP, przez kody smsowe czy e-mail.*

Apple po ataku, zaleciło swoim klientom korzystanie z silnych haseł zabezpieczających, a także wykorzystanie systemu dwuetapowego uwierzytelniania, aby maksymalnie utrudnić atak na konta iCloud. Jednak według australijskiego programisty, Nika Cubrilovika, system dwuetapowego uwierzytelniania nie jest w stanie uchronić użytkowników przed ściągnięciem przez hakerów ich zdjęć czy filmów, ponieważ system chroni jedynie dane i uaktualnienia, a nie kopię zapasową.

*Dwuetapowe uwierzytelnianie dla iCloud jest bezużyteczne w ochronie haseł czy tokenów autoryzacyjnych, wykorzystywanych do odzyskiwania kopii zapasowych* – twierdzi Cubrilovik.

Jedna z ofiar hakerów, aktorka Mary Winstead znana głównie z filmu *Just Dance* i dwóch ostatnich odsłon *Szklanej Pułapki*, twierdzi, że zdjęcia skradzione z jej konta zostały przez nią dawno temu usunięte. Jak zatem hakerzy uzyskali dostęp do usuniętych zdjęc?

Potencjalnym wyjaśnieniem może być to, że zdjęcia zostały skradzione jakiś czas temu, ale dopiero niedawno zostały opublikowane na portalu **4chan**. W tę hipotezę nie wierzy jednak **Moit Sagey – strateg bezpieczeństwa informacji Check Pointa**, który od momentu umieszczenia przez aktorkę wpisu, zaczął interesować się sprawą.

Sagey podczas analizy iCloud odkrył, że usługa przechowuje nie jedną, a nawet do trzech pełnych kopii zapasowych. Każda z nich zachowana jest do momentu zastąpienia jej przez nową kopię, jednak dzieje się tak dopiero, gdy użytkownik synchronizuje swoje użądzenie przez komputer podłączony do źródła zasilania i Internetu. W związku z tym iCloud może przechowywać poprzednie kopie plików przez dłuższy czas.

źródło: twitter.com/M\_E\_Winstead

*Mogą minąć tygodnie lub nawet całe miesiące pomiędzy zmianami w backupie, więc zdjęcia usunięte z urządzenia mogą być wciąż dostępne w jednej z wcześniejszych kopii zapasowych*. *Jeżeli haker uzyskał nazwę użytkownika i hasło dla iCloud, może użyć takiego narzędzia jak Dr. Fone, by odzyskać dane z trzech wersji kopii zapasowych, w tym treści usunięte przez użytkownika* – powiedział Moit Sagley.

*Jestem pewien, że hakerzy wiedzieli, że istnieją 3 wersje backupów lub z pomocą odpowiednich narzędzi odkryli to przypadkiem* – zakończył ekspert Check Pointa.

Dodatkowe dwie kopie zapasowe miały zapewne służyć jako zwykłe udogodnienie w przypadku, gdy pliki nie zostaną prawidłowo przetransferowane na serwery. Architektura Apple’a nie była więc w założeniu zła. Użytkownicy powinni być jednak świadomi, że samo usunięcie pliku z urządzania z systemem iOS nie oznacza, że go nie ma w iCloud.