Bitdefender

Oprogramowanie szpiegujące QuaDream Reign atakuje właścicieli iPhonów

13.04.2023

Oprogramowanie szpiegujące QuaDream Reign atakuje właścicieli iPhonów, w szczególności polityków, celebrytów i inne osoby publiczne, już od 2021 roku, jednak w ostatnim czasie badacze bezpieczeństwa odkryli nowe dowody, że zagrożenie to jest nadal aktualne i wciąż zagraża użytkownikom smartfonów Apple.

W raporcie opublikowanym w tym tygodniu badacze z Citizen Lab z University of Toronto zidentyfikowali co najmniej pięć ofiar, których smartfony zostały zainfekowane oprogramowaniem szpiegującym Reign opracowanym przez izraelską firmę QuaDream.

Nowa kampania hakerska

Wśród celów byli między innymi dziennikarze, działacze opozycji politycznej i pracownicy organizacji pozarządowych w Ameryce Północnej, Azji Środkowej, Azji Południowo-Wschodniej, Europie i na Bliskim Wschodzie.

Lokalizacje operatorów systemów QuaDream znaleziono w Bułgarii, Czechach, na Węgrzech, w Ghanie, Izraelu, Meksyku, Rumunii, Singapurze, Zjednoczonych Emiratach Arabskich i Uzbekistanie.

Eksperci do spraw cyberbezpieczeństwa zidentyfikowali ślady podejrzanego exploita typu zero-click w iOS 14, który został wdrożony jako zero-day przeciwko iOS w wersjach 14.4 i 14.4.2 oraz prawdopodobnie w innych wersjach.

Exploit, nazwany ENDOFDAYS, ma wykorzystywać niewidoczne zaproszenia z kalendarza iCloud wysyłane do ofiar przez operatora oprogramowania szpiegującego.

- Oprogramowanie szpiegujące może podobno:
- Nagrywać dźwięk z rozmów telefonicznych
- Nagrywać dźwięk z mikrofonu
- Robić zdjęcia przednią lub tylną kamerą urządzenia
- Eksfiltrować i usuwać elementy z pęku kluczy urządzenia

- Generować hasła iCl0oud 2FA
- Uruchamiać zapytania w bazach danych SQL w telefonie
- Śledzić lokalizację urządzenia
- Wykonywać operacje w systemie plików, w tym wyszukiwać pliki o określonych cechach
- Czyścić pozostałości pozostawione przez exploity typu zero-click

Ponadto w poradniku przygotowanym przez badaczy Microsoftu zauważono, że „przechwycone próbki dotyczyły urządzeń z systemem iOS, w szczególności iOS 14, ale istniały przesłanki, że część kodu może być również używana na urządzeniach z Androidem."

Badacze Microsoftu twierdzą, że niektóre techniki użyte w tej próbce mogą już nie działać w nowszych wersjach systemu operacyjnego, ale ostrzegają, że QuaDream najprawdopodobniej zaktualizuje (lub już zaktualizowało) swoje złośliwe oprogramowanie tak, aby było kompatybilne z nowszym modelami systemów operacyjnych.

QuaDream Reign atakuje właścicieli iPhonów – jak się bronić?

„Obecnie ataki spyware są wysoce ukierunkowane. Dlatego zespół Bitdefender zdecydowanie zaleca wszystkim użytkownikom smartfonów regularne aktualizowanie telefonów komórkowych, aby ograniczyć

ryzyko infekcji złośliwym oprogramowaniem poprzez exploity dnia zerowego. Oprócz tego musimy pamiętać o zabezpieczeniu swojego urządzenia skutecznym oprogramowaniem antywirusowym. Niestety czasy, w których użytkownicy smartfonów z systemami iOS mogli cieszyć się względnym cyberbezpieczeństwem bez korzystania z oprogramowania zabezpieczającego, już minęły. Kampanie takie jak ta z wykorzystaniem QuaDream Reign tylko to potwierdzają" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Firma Apple niedawno podłączyła dwa nowe systemy operacyjne typu zero-day zarówno do swoich mobilnych, jak i stacjonarnych systemów operacyjnych, w tym do iPhone'ów starej generacji, co wydaje się skoordynowanym wysiłkiem mającym na celu powstrzymanie oprogramowania szpiegującego.

W listopadzie 2021 roku producent iPhone'a pozwał izraelską grupę twórców oprogramowania szpiegującego NSO w związku ze złośliwym oprogramowaniem Pegasus.

W odpowiedzi na falę ataków spyware wymierzonych w iOS gigant technologiczny z Cupertino wprowadził ustawienie trybu blokady, który zmniejsza powierzchnię ataku platformy. Jednak niezależnie od modelu urządzenia lub wersji systemu operacyjnego ważne jest wdrożenie dedykowanego rozwiązania antywirusowego, aby przez cały czas chronić się przed zagrożeniami w sieci.

Źródło: https://bitdefender.pl/oprogramowanie-szpiegujace-quadream-

reign-atakuje-wlascicieli-iphonow/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 13.04.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.