**WhatsApp stał się furtką do zainfekowania urządzeń mobilnych!**

**WhatsApp poinformował ponad 1,5 miliarda użytkowników na całym świecie o konieczności aktualizacji aplikacji, uzasadniając to względami bezpieczeństwa. Przyczyną był atak skierowany na "wybraną liczbę" użytkowników, który został przeprowadzony przez "zaawansowanego hakera lub organizację hakerską” – poinformował brytyjski serwis BBC.**

*- Praktycznie każdy użytkownik tej aplikacji mógł być zagrożony, tym bardziej jeśli złośliwe oprogramowanie wykorzystane byłoby przez organizacje przestępcze* – podkreśla Oded Vanunu, szef badań i produktów w firmie Check Point Software Technologies.

Teraz atakujący korzystali z funkcji wywołania głosowego WhatsApp, aby zadzwonić do urządzenia docelowego. Malware uruchamiał się nawet, gdy połączenie nie zostało odebrane. Z doniesień dziennika Financial Times wynika, że dla wielu użytkowników WhatsApp atak mógł być niewidoczny, ponieważ samo połączenie często znikało z dziennika połączeń telefonu. Tymczasem wirus kopiował wiele, poufnych danych z telefonu lub urządzenia poszkodowanego.

*Atak ma wszystkie cechy charakterystyczne dla prywatnej firmy, która podobno współpracuje z rządami w celu dostarczenia oprogramowania szpiegującego, które przejmuje funkcje systemów operacyjnych dla telefonów komórkowych* – poinformowała firma CoApp, która wykryła incydent. Łatka naprawiająca podatność została już udostępniona przez WhatsApp.

Financial Times uważa, że technika i metoda ataku zostały opracowane przez izraelską firmę cyberwywiadowczą NSO Group.

O kłopotach WhatsApp było głośno w kwietniu br. gdy zaatakowano i wykradziono tajne dane z telefonu prezydenta Ekwadoru. Już wówczas zwracano uwagę, że WhatsApp ma luki i niedociągnięcia pozwalające uzyskać dostęp do wiadomości pomimo zastosowanego szyfrowania end-to-end.

Analitycy portalu AvLab.pl zwracają uwagę, że dotychczas jedynie UseCrypt Messenger pozwala na realne zabezpieczanie rozmów i samego urządzenia. Jak dotąd nie doszło do ani jednego przypadku ujawnienia tożsamości rozmówców albo kradzieży kontaktów, wiadomości, załączników, kluczy kryptograficznych itp. Prawdopodobnie ta myśl techniczna wyprzedza o jeden krok wszystkie dostępne na rynku komunikatory

**Jak działa skuteczna aplikacja?**

Zaawansowany i bezpieczny komunikator powinien posiadać wbudowany moduł pozwalający wykryć zainstalowane złośliwe oprogramowanie, które mogłoby przechwytywać dane z naszego urządzenia przed rozpoczęciem rozmowy. Aplikacja winna posiadać „pierwszeństwo” (brak nieautoryzowanego dostępu) do mikrofonu, głośnika oraz aparatu. W przypadku stwierdzenia ataku, uniemożliwi wykonanie połącznia i wymusi jej zamknięcie.

**Komentarz eksperta:**

*- Wielu użytkowników, również na poziomie rządowym, przyjmuje za pewnik, że darmowe komunikatory oferujące połączenia w tzw. protokole „end-to-end” skutecznie szyfrują połączenia głosowe. Ta historia pokazuje, że oprogramowanie szpiegowskie działa na poziomie mikrofonu, zanim aplikacja ma szansę zaszyfrować dźwięk* – mówi Wojciech Głażewski, dyrektor generalny firmy Check Point w Polsce.

*Źródła:*

<https://www.bbc.com/news/technology-48262681/>

[*https://avlab.pl/wszystko-co-musicie-wiedziec-o-komunikatorze-usecrypt-messenger*](https://avlab.pl/wszystko-co-musicie-wiedziec-o-komunikatorze-usecrypt-messenger)