aut. Szymon Palczewski 30.03.2020

KAMPANIA CYBERSZPIEGOWSKA W HONGKONGU. MASOWA KRADZIEŻ DANYCH

Specjaliści ds. cyberbezpieczeństwa zidentyfikowali nową kampanię hakerską, która miała miejsce w Hongkongu. Głównym zamiarem cyberprzestępców było zainfekowanie jak największej ilości urządzeń w celu gromadzenia danych. Czy złośliwe działania należy traktować jako odpowiedź Państwa Środka na protesty lokalnych działaczy przeciwko kontrowersyjnemu chińskiemu prawu ekstradycyjnemu?

Specjaliści ds. cyberbezpieczeństwa firmy TrendMicro oraz Kaspersky Lab wykryli nową serię cyberataków wymierzonych w mobilne systemy iOS oraz Android, która miała miejsce na terenie Hongkongu. Złośliwe oprogramowanie umożliwiało hakerom przejęcie kontroli nad urządzeniami oraz uzyskanie dostępu do takich danych, jak lokalizacja GPS, połączenia telefoniczne, kontakty czy wiadomości tekstowe.

Według ekspertów firmy TrendMicro kampania wykorzystuje złośliwe linki, które są zamieszczane na określonych forach internetowych. „Użytkownicy, którzy klikną w link pobiorą na swoje urządzenie nową wersję złośliwego oprogramowania" – czytamy w oficjalnym komunikacie TrendMicro. Wirus został nazwany przez specjalistów „lightSpy".

Analiza kampanii wykazała, że złośliwe oprogramowanie umożliwia hakerom prowadzenie operacji szpiegowskich. Cyberprzestępcy mogą bez problemów przejąć kontrolę nad zainfekowanym urządzeniem, uzyskując dostęp do danych. Eksperci TrendMicro podkreślają, że celem kampanii jest zainfekowanie jak największej ilości urządzeń.

„Podsumowując, wirus pozwala hakerom dogłębnie spenetrować zaatakowane urządzenia i uzyskać dostęp do większości danych, które użytkownik traktuje jako poufne" – wyjaśniają specjaliści TrendMicro. – „Kilka aplikacji czatowych popularnych na rynku w Hongkongu było wykorzystanych podczas kampanii, co sugeruje, że ich użytkownicy byli głównym celem operacji".

Z kolei Kaspersky wskazuje, że pierwsze przesłanki na temat incydentu zostały odkryte na początku bieżącego roku. Specjaliści tłumaczą, że kampania została specjalnie zaprojektowana z myślą o użytkownikach znajdujących się w Hongkongu. Do takiej tezy prowadzi analiza zawartości strony docelowej. „Grupę odpowiedzialną za cyberataki nazwaliśmy >TwoSail Junk<" – czytamy na oficjalnej stronie Kaspersky Lab.

Specjaliści podkreślają, że złośliwe oprogramowanie było rozpowszechniane między innymi za pomocą postów na Instagramie. Hakerzy zachęcali użytkowników do klikania w link odwołując się do istotnych wydarzeń, mających miejsce w Hongkongu. Wśród nich poruszono kwestię protestu lokalnych działaczy przeciwko kontrowersyjnemu chińskiemu prawu ekstradycyjnemu, które było wspierane przez kampanie inwigilacyjne i dezinformacyjne.