

WAKACJE POD PALMĄ? CYBERPRZESTĘPCY PRZEJMUJĄ DANE KLIENTÓW POPULARNYCH HOTELI

Dane turystów korzystających w ostatnim czasie z hotelów, hosteli oraz firm turystycznych mogą być zagrożone – twierdzą eksperci. Firma Kaspersky wykryła złośliwą kampanię wymierzoną w głównie w obiekty turystyczne zlokalizowane w Brazylii, ale także w innych popularnych wśród Polaków kierunkach jak Hiszpania, Tajlandia, Turcja, Francja, Włochy, Portugalia, Argentyna, Boliwia, Chile, Kostaryka czy Meksyk.

Kampania grupy nazwanej przez ekspertów jako RevengeHotels została wymierzona w celu przechwycenie danych kart kredytowych gości, przechowywanych w systemach hotelowych, a także danych otrzymanych od popularnych internetowych pośredników takich jak Booking.com. Ataki odbywają się głównie za pośrednictwem poczty elektronicznej z dołączonymi spreparowanymi dokumentami Word, Excel lub PDF. Grupa odpowiedzialna za ataki jest aktywna od 2015 roku, ale odnotowano znaczny wzrost liczby ataków w 2019 roku.

Schemat działania jest dość prosty. Cyberprzestępcy proszą o wycenę rezerwacji dla dużej liczby osób podając się za jednostkę rządową lub prywatną firmę. Grupa rejestruje domeny zawierające literówki podszywając się pod legalne firmy czy instytucje, dlatego też pracownicy sprawdzający informacje o nadawcy mogą „potwierdzić” w sieci informacje o nadawcy. Dla uwiarygodnienia, maile zawierają dużą ilość informacji potrzebnych do uśpienia czujności pracownika hotelu.

Po pozyskaniu dostępu, cyberprzestępcy mieli możliwość zbierania danych ze schowka, bufora drukarki oraz przesłanie zrzutów z ekranu. Eksperci Kasperskiego odnotowali również przypadki sprzedaży również danych uwierzytelniających do zainfekowanych systemów innym hakerom.

Zidentyfikowano dwie grupy odpowiedzialne za prowadzenie kampanii, korzystającej z oddzielnej, ale zdaniem ekspertów podobnych narzędzi i technik. Pierwszą z nich nazwaną podobnie jak nazwę kampanii RevengeHotels natomiast drugą ProCC.

W toku monitorowania aktywności tych grup, wykryto również trzecią jednostkę, jednak nie jest na ten moment jasne czy koncertuje się ona wyłącznie na sektorze hotelarskim lub czy jest to jedynie ich poboczna działalność.

Najwięcej ofiar zlokalizowano w Brazylii, Stanach Zjednoczonych i Portugalii. Ale ataki nie ominęły również innych popularnych kierunków jak Hiszpania, Austria, Chiny, Francja, Maroko, Korea, Holandia, Tajlandia, Turcja czy Dominikana.