Cyberdefence 24

aut. Szymon Palczewski 13.08.2020

ROSYJSCY HAKERZY UDERZYLI W NAJWIĘKSZE KORPORACJE. PHISHING NA ŚWIATOWĄ SKALĘ

Rosyjscy hakerzy od co najmniej 2018 roku prowadzili kampanie spear-phishingowe wymierzone w korporacje z całego świata. Ich działalność odznaczała się wysoką dbałością o szczegóły przez co wielu użytkowników dało się „nabrać" na sztuczki hakerskie. Specjaliści wskazują, że jest to nieznana dotąd grupa, której członkami są Rosjanie.

Specjaliści firmy Group-IB nazwali nową grupę rosyjskich hakerów „RedCurl". Według przeprowadzonych badań od 2018 roku prowadziła kampanie cyberszpiegowskie, wymierzone głównie w korporacje, w celu kradzieży tajemnic handlowych i danych osobowych pracowników. Jej głównym obiektem zainteresowania były firmy z całego świata – donosi serwis ZDNet.

Eksperci Group-IB śledzą działalność grupy od połowy 2019 roku, kiedy to po raz pierwszy poproszono ich o zbadanie incydentu w jednej ze zhakowanych firm. Od tego czasu specjalistom udało się zidentyfikować 26 innych cyberataków przeprowadzonych przez RedCurl. Najwcześniejszy miał miejsce w 2018 roku.

Ofiary rosyjskich hakerów różniły się w zależności od państw i sektorów, w jakich działały poszkodowane podmioty. Były to między innymi przedsiębiorstwa budowlane, biura podróży, firmy ubezpieczeniowe, banki oraz podmiotu prawnicze i konsultingowe z takich krajów jak Rosja, Ukraina, Kanada, Niemcy, Norwegia i Wielka Brytania.

Podczas złośliwych kampanii grupa nie posługiwała się skomplikowanymi narzędziami ani zaawansowanymi technikami hakerskimi. Hakerzy bazowali głównie na spear-phishingu w celu uzyskania dostępu do sieci i systemów ofiary.

„Charakterystyczną cechą RedCurl jest jednak to, że treść wiadomości e-mail jest starannie przygotowana" – wskazali specjaliści Group-IB, cytowani przez ZDNet. Przykładowo rozsyłane wiadomości zawierały adres i logo firmy docelowej, podczas gdy dane nadawcy uwzględniały nazwę domeny przedsiębiorstwa.

„Atakujący udawali członków zespołu HR w zaatakowanej organizacji i wysyłali e-maile do wielu pracowników jednocześnie, co zmniejszyło ich czujność, zwłaszcza biorąc pod uwagę, że wielu z nich pracowało w tym samym dziale" – podkreślili eksperci.

W treści wiadomości zawarte były załączniki ze złośliwym oprogramowaniem. Po ich uruchomieniu na nośnikach ofiary hakerzy instalowali trojany, które zapewniały im dostęp do podstawowych operacji, takich jak przeglądanie systemów czy przesyłanie skradzionych plików na zdalne serwery.

Rosyjscy hakerzy próbowali również rozprzestrzenić złośliwe oprogramowanie na inne systemy za pomocą powiązań występujących między sieciami. Co więcej, grupa starała się ukryć swoje działania i

nie wykonywała gwałtownych, nieprzemyślanych ruchów. „Faza rozprzestrzeniania się w sieci jest znacznie wydłużona w czasie, ponieważ hakerzy starają się pozostać niezauważeni tak długo, jak to możliwe” – wyjaśnili eksperci Group-IB, cytowani przez ZDNet.

Czytaj też: Rosyjski wywiad poluje na szczepionkę przeciwko Covid-19