aut. Szymon Palczewski 13.12.2019

HAKERZY PRZEJMUJĄ KONTA UŻYTKOWNIKÓW TELEGRAMA. ROSYJSCY PRZEDSIĘBIORCY OFIARAMI

Hakerzy przejmują kody uwierzytelniające do Telegrama, uzyskując dostęp do pełnej korespondencji. Jednym z głównych celów cyberprzestępców są rosyjscy przedsiębiorcy oraz osoby ze środowiska naukowego. Kampania nadal trwa, dlatego wszyscy użytkownicy aplikacji powinni wprowadzić dodatkowe zabezpieczenia swoich kont. Gdzie trafiają przejęte wiadomości i konta?

Podczas kampanii hakerzy przechwycili kody wykorzystywane przez użytkowników do uwierzytelniania konta w aplikacji Telegram. Mechanizm weryfikacji jest prosty. Za każdym razem, gdy dochodzi do logowania na nowym urządzeniu, na telefon komórkowy konkretnej osoby wysyłany jest SMS, w którego treści znajduje się kod, przeznaczony do weryfikacji zgodności.

Według specjalistów grupy IB w ramach złośliwej kampanii cyberprzestępcy zdołali uzyskać dostęp do niektórych rosyjskich kont popularnej aplikacji, pobierając z nich całą korespondencję. Jednym z poszkodowanych użytkowników jest Dmitri Rodin, przedstawiciel środowiska naukowego. W rozmowie z Forbes podkreślił, że 1 grudnia otrzymał ostrzeżenie wysłane przez Telegram, które wskazywało, że ktoś z zewnątrz próbuje się zalogować na jego konto. Mężczyzna początkowo odrzucił powiadomienie, jednak po otrzymaniu kolejnego natychmiast podjął działania. Wówczas okazało się, iż cyberprzestępcy skutecznie zalogowali się na jego profil.

Dmitri Rodin po wykryciu nieprawidłowości od razu przeszedł do ustawień aplikacji i aktywował dodatkowe hasło jako kolejną warstwę uwierzytelniania. W wywiadzie dla Forbes specjalista zalecił, aby wszyscy użytkownicy Telegrama zrobili to samo ze względów bezpieczeństwa.

Mężczyzna uważa, że hakerzy niekoniecznie musieli wykryć, a następnie wykorzystać luki w aplikacji, aby przejąć konto. „To nie musi być problem Telegrama” – zaznaczył Dmitry Rodin. „Być może ktoś zalogował się na moje konto, przechwytując SMS, co sugeruje, że może istnieć problem ze strony operatora telekomunikacyjnego”. W związku z tym zagrożone cyberatakiem są również wszystkie inne konta, wykorzystujące SMS jako środek uwierzytelniający.

Grupa IB otrzymała dotychczas 13 zgłoszeń o podobnych naruszeniach. Należy się jednak spodziewać, że liczba ta prawdopodobnie wzrośnie, ponieważ jest to nowa kampania, która dopiero zaczyna się rozprzestrzeniać.

Typ cyberataku

Dla przeciętnego użytkownika Telegramu lub każdej osoby korzystającej z innej aplikacji, która wysyła kody SMS do logowania, najbardziej niepokojące jest to, że hakerzy mogli uzyskać dostęp do tych danych uwierzytelniających w pierwszej kolejności. Na razie niewiadomo, w jaki sposób działali

cyberprzestępcy.

Specjaliści wskazują, że w ostatnich latach nastąpił wzrost liczby podobnych incydentów. Cyberprzestępcy interesują się siecią telekomunikacyjną, ponieważ skuteczny atak umożliwia im pobranie treści wiadomości bez ingerencji w urządzenie ofiary.

Czarny rynek

Nielegalny handel danymi do logowania, takich aplikacji jak Telegram, z roku na rok rośnie. Jak informuje Forbes, na czarnym rynku (na przykład forum Hydra) hakerzy oferują pełny dostęp do konta nawet za 3900 dolarów. Spotkać się można również z ofertami sprzedaży danych do aplikacji WhatsApp oraz innych poufnych informacji, których cena waha się od 1550 dolarów do 5450.

Czytaj też: Polscy prokuratorzy na celowniku cyberprzestępcy. Prywatne dane i służbowe dokumenty w sieci