Cyberdefence 24

aut. Tomasz Fastyn 09.06.2016

32 MILIONY DANYCH LOGOWANIA DO TWITTERA W RĘKACH HAKERÓW

Kolejny wyciek danych z dużego portalu społecznościowego pokazuje, że nadal nie dbamy o bezpieczne hasła. Bazę 32 mln rekordów zawierających hasła dostępu do Twittera przekazał stronie Leakedsource jeden z użytkowników portalu.

Leakedsource to portal, na którym możemy znaleźć informacje o wyciekach z popularnych serwisów internetowych. Ostatnio Leakedsource udostępnił informacje o kontach zarejestrowanych na portalu Twitter. Użytkownik portalu o pseudonimie „Tessa88@exploit.im" znalazł je w Mrocznej Sieci, gdzie najpewniej hakerzy oferują ich sprzedaż.

Wyciek ponad 32 mln danych do logowania na portalu społecznościowym Twitter pokazuje, że proste hasła nadal są w modzie. Wśród haseł przeanalizowanych przez portal leakedsource.com w pierwszej piątce są hasła naprawdę łatwe do złamania. Chodzi o takie hasła jak *123456* występujące ponad 120 tys. razy czy *123456789*, *qwerty, password* oraz *1234567*.

Jak dalej wynika z analizy bazy danych, znaczna część adresów e-mail pochodzi z terenów Rosyjskich. Prawie 7 mln adresów posiadało rozszerzenie .ru, jedna bardziej niepokojącą jest informacja, że ponad 3 tys. adresów e-mail miało końcówkę .gov.

Wyciek najpewniej nie był wynikiem ataku na portal Twitter albo przejęciem baz danych logowania z serwera należącego do serwisu. Według strony Leakedsource dostęp do danych logowania został uzyskany przez złośliwe oprogramowanie, które zaatakowało przeglądarki na kontach użytkowników Twittera. Ma to wynikać z tego, że przeglądarki Google Chrome oraz Firefox przechowują hasła w swoich bazach w postaci czystego tekstu, nie zabezpieczonego w żaden sposób.

Rzecznik prasowy firmy Twitter potwierdził informacje, o tym, że żadne bazy danych na portalu nie zostały zaatakowane - "Jesteśmy pewni tego, że hasła oraz nazwy użytkowników nie zostały zdobyte w wyniku włamania do baz danych Twittera. Staramy się pomagać użytkownikom naszego serwisu w sprawie bezpieczeństwa ich kont. Sprawdzamy poprzednie wycieki danych logowania i analizujemy ją z naszą bazą użytkowników".

Portal Techchrunch podchodzi sceptycznie do tych informacji. Według dziennikarzy jest szansa, że część informacji udostępnionych w tym wycieku jest fałszywa, a część pochodzi z innych ataków.

Czy wyciek jest do końca prawdziwy, tego nikt nie jest wstanie potwierdzić. Jedyne co dziś wydaje się dobrym pomysłem to zmiana hasła lub skorzystanie z usług menadżera haseł. Ważne, by hasło było bardziej skomplikowane niż *123456.*

Czytaj też: Podatność Facebook Messengera pozwala przejąć wiadomości użytkowników