Gmina Mielec
ul. Głowackiego 5, 39-300 Mielec
Godziny pracy Urzędu: pon.: 7:30 - 17:00, Wt. - Czw.: 7:30 - 15:30, Pt.: 7:30 - 14:00
Telefon: 17 773 05 90 Fax: 17 773 05 91 Email: sekretariat@ug.mielec.pl

Ostrzeżenie CERT Polska o spersonalizowanych atakach na ofiary wycieków

2023-01-11 12:54:09

Pełna treść ostrzeżenia dostępna w komunikacie "Spersonalizowane ataki na ofiary wycieków" na stronie CERT.

- **Szczególnie narażeni użytkownicy: Ofiary wycieków**
- **Wektor ataku: Wiadomości na portalach społecznościowych, komunikatorach oraz serwisach pocztowych**
- **Możliwe skutki: Utrata poczucia bezpieczeństwa oraz środków pieniężnych**
- **Atakowane platformy: Różne**

Schemat działania

1. **Znalezienie potencjalnych ofiar**
   Przestępcy coraz częściej personalizują swoje kampanie pod potencjalne ofiary, czym chcą wzbudzić ich większe zaniepokojenie, ale także urealistycznić atak. Osiągają to m.in. zwracając się do adresata bezpośrednio po jego imieniu. Dane takie zostały najczęściej upublicznione w ramach wycieku lub zostały pozyskane poprzez web scrapping, czyli zebrane automatycznie z serwisów, na których były dostępne publicznie.
2. **Szantaż**
   Po nawiązaniu kontaktu oszust próbuje zmusić ofiarę do wykonania określonych przez niego czynności, w przeciwnym wypadku rzekomo upubliczni kompromitujące poszkodowanego zdjęcia lub nagrania. Najczęściej przestępcy żądają przelania wyznaczonej sumy pieniędzy na portfel kryptowalutowy, natomiast w ostatniej zaobserwowanej przez nas kampanii, szantażyści namawiali kobiety do wejścia na ich stronę internetową.
3. **Serwis internetowy**
   Po wejściu i zarejestrowaniu się na stronie internetowej, dochodziło do bezpośredniej rozmowy, w trakcie której oszuści próbowali wymusić na poszkodowanych przesłanie rzeczywistych zdjęć o charakterze erotycznym.

Skutki oszustwa

Podjęcie komunikacji oraz udostępnienie zdjęć skutkowałoby najprawdopodobniej kolejnymi szantażami oraz próbą wyłudzenia środków pieniężnych. Należy zauważyć, że jakiekolwiek próby podejmowania rozmowy czy negocjacji z przestępcami eskalują potencjalny konflikt i prowadzą jedynie do coraz to większych żądań.

Jak się chronić?

Ważnym elementem ochrony jest budowanie świadomości w kwestii źródeł pozyskiwania danych na temat ofiar przez przestępców.

Każdy, kto dokonuje zakupów w sklepach internetowych albo korzysta z mediów społecznościowych, może paść ofiarą wycieku danych osobowych, a następnie próbie szantażu, kiedy to przestępca powiąże jego dane z numerem telefonu czy też adresem e-mail. Należy jednak zauważyć, że oszuści posiadają zazwyczaj niewiele danych, które nie są w dodatku wcale danymi wrażliwymi.

Co zrobić w przypadku, gdy padło się ofiarą?

W tym przypadku zalecamy podjąć następujące kroki:

- **zgłosić fakt szantażu na najbliższym komisariacie Policji**
- **nie podejmować korespondencji z przestępcą**
- **podejrzane wiadomości SMS, zawierające adres URL, przekazać nam na numer 799-448-084, a wszelkie inne zagrożenia zgłosić za pomocą formularza na stronie Zgłoś incydent CERT.PL.**

Dziękujemy za odwiedziny i zapraszamy ponownie

bezpośredni link do strony www