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

Komunikat CERT Polska w sprawie publikacji zbioru wykradzionych danych do logowania

2023-06-01 07:42:34

Pełna treść informacja dostępna w komunikacie "Publikacja zbioru wykradzionych danych logowania - co zrobić?" na stronie CERT.

W tym tygodniu doszło do publikacji dużego zbioru danych wykorzystywanych do logowania przez polskich użytkowników. W ramach tego wycieku udostępniono ponad milion unikalnych rekordów z loginem oraz hasłem do różnych stron. W związku z tym jednostki odpowiedzialne za cyberbezpieczeństwo w Polsce, w tym CERT Polska, podjęły odpowiednie działania w celu ograniczenia skutków tej sytuacji.

Jak przestępcy uzyskali dostęp do danych logowania

W trakcie analizy zbioru danych, zespół CERT Polska wykazał, że dane znajdujące się w wycieku są złączeniem wielu mniejszych zbiorów pozyskanych przez złośliwe oprogramowanie typu "information stealer".
W związku z tym, przestępcy mogli mieć dostęp zarówno do haseł wpisywanych na klawiaturze i mieli dostęp do danych logowania zapisanych w przeglądarkach czy menedżerach haseł.

Jakie kroki podjął nasz zespół

Oprócz analizy danych znajdujących się w wycieku, nasz zespół podjął się również działań, które miały na celu powiadomienie jak największego grona odbiorców. Udostępniliśmy informacje na temat upublicznionych kont użytkownikom systemu n6 oraz powiadomiliśmy mailowo wiele instytucji, w szczególności administratorów rozpoznawalnych skrzynek pocztowych. Na moment pisania artykułu przesłaliśmy powiadomienia dotyczące ponad miliona unikalnych maili oraz loginów. Dodatkowo udostępniliśmy upublicznione dane portalom HIBP oraz Bezpieczne Dane, które umożliwiają każdemu weryfikację czy dane konto lub email pojawił się w wycieku.

Jak możecie sprawdzić czy Wasze konto znalazło się w wycieku

W związku z dużą skalą wycieku, zachęcamy Was do sprawdzenia, czy Wasze dane znajdują się w upublicznionym zbiorze. Nasz zespół zasilił dwa serwisy internetowe w dane z wycieku, dzięki czemu możecie zweryfikować czy padliście ofiarą tego zdarzenia.

Możecie to zrobić na stronach:

- **bezpiecznedane.gov.pl - serwis stworzony przez COI, który po zalogowaniu poprzez Profil Zaufany umożliwia zweryfikowanie czy dane konto lub email znalazło się w wycieku. Na obecną chwilę w tym serwisie dostępne są dane wyłącznie ze wspomnianego wcześniej incydentu.**
- **haveibeenpwned.com - popularny serwis stworzony przez Troya Hunta, który od lat umożliwia zweryfikowanie czy Wasze konto padło ofiarą większych wycieków. Co więcej, strona ta pozwala zweryfikować informacje na temat wycieków odnośnie całej nazwy domeny, co może być użyteczne dla wielu firm, chcących sprawdzić skalę wycieku w swojej organizacji,**

Jak się chronić?

- **Nie ulegać presji czasu i autorytetu – to właśnie dzięki wpłynięciu na emocje oszuści chcą skłonić ofiarę do szybkiego, nieprzemyślanego działania.**
- **Wprowadzić filtry antyspamowe – chociaż w wielu przypadkach pełne odfiltrowanie takich szkodliwych wiadomości nie będzie możliwe, to oznaczanie wiadomości przychodzących z nieznanych źródeł może wzmóc czujność.**
- **Weryfikować – zweryfikowanie żądania zmiany numeru konta czy wykonania przelewu innymi kanałami niż otrzymana wiadomość pozwoli wykryć próbę oszustwa.**

Co możecie zrobić, jeżeli Wasze dane są w wycieku (lub chcecie poprawić bezpieczeństwo swojego konta)

Zachęcamy do podjęcia następujących kroków:

1. **Użyjcie programu antywirusowego, żeby sprawdzić bezpieczeństwo swojego komputera. Należy jednak zwrócić uwagę, że antywirusy mogą nie wykryć zagrożenia. Jeżeli zatem zachodzi podejrzenie, że system może być zainfekowany, najlepiej zabezpieczyć najważniejsze dane i przywrócić go do stanu fabrycznego,**
2. **Korzystając z zabezpieczonego lub wyczyszczonego komputera zmieńcie hasła do logowania, których używaliście dotychczas.**
   Ważne! Jeśli do logowania na różnych serwisach wykorzystywaliście to samo hasło, zmieńcie je również na pozostałych stronach! Nie powielajcie też haseł między serwisami!,
3. **Włączcie dodatkowe zabezpieczenie w serwisach, które umożliwiają weryfikację dwuetapową,**
4. **Zwróćcie szczególną uwagę na próby logowania na konta, sprawdzajcie alerty przesyłane na adres e-mail.**

Informacje na temat najnowszych zagrożeń można znaleźć śledząc profile zespołu CERT Polska na Facebooku albo Twitterze.

Dziękujemy za odwiedziny i zapraszamy ponownie

bezpośredni link do strony www