Image not found or type unknown

Komunikat CSIRT CeZ - ostrzeżenie przed nową, zaawansowaną kampanią cyberprzestępczą

CSIRT CeZ ostrzega przed nową, zaawansowaną kampanią cyberprzestępczą wymierzoną w lekarzy oraz osoby uprawnione do wystawiania recept. Atakujący podszywają się pod przedstawicieli instytucji publicznych, np. NFZ, ZUS oraz rzekome zespoły cyberbezpieczeństwa i wykorzystują techniki socjotechniczne, aby przejąć dane uwierzytelniające, certyfikaty e-ZLA oraz dostęp do aplikacji gabinetowych.
W efekcie dochodzi do nieuprawnionego dostępu do wrażliwych danych osobowych pacjentów oraz wystawiania recept na leki psychotropowe i narkotyczne bez wiedzy lekarza.
Poniżej prezentujemy scenariusz ataku i najważniejsze wskazówki, jak zminimalizować zagrożenie.
Ważne! Zgłoś incydent do CSIRT CeZ
Jeśli zauważyli Państwo podejrzaną aktywność, otrzymali nietypowy telefon, SMS lub e-mail – prosimy o niezwłoczne zgłoszenie incydentu poprzez formularz CSIRT CeZ:
https://cez.gov.pl/pl/page/zglos-incydent
Wczesna reakcja pozwala zapobiegać dalszym nadużyciom i chronić cały sektor ochrony zdrowia.

Jak wygląda atak?
1. Telefon od fałszywego pracownika instytucji
Cyberprzestępcy dzwonią z różnych numerów, przedstawiając się jako pracownicy NFZ lub zespołów ds. cyberbezpieczeństwa. Często używają nazwisk „Tomasz Zieliński” lub „Tomasz Ochocki” i informują o rzekomo wystawionych receptach na leki, np. Oxydolor.
2. Odesłanie na fałszywą stronę
Ofiara proszona jest o wejście na witryny:

- eincydent[.]org
- e-incydent[.]org
- m-incydent[.]org
- podobne do powyższych

Strony są stylizowane na serwisy instytucji publicznych i mają rzekomo służyć „zabezpieczeniu konta” lub „zgłoszeniu incydentu”.
Prawdziwe incydenty zgłaszaj wyłącznie przez stronę CSIRT CeZ.
3. Logowanie przez aplikację mObywatel
Na stronie ofiara proszona jest o uwierzytelnienie się przez mObywatela, co umożliwia cyberprzestępcom pozyskanie dodatkowych danych osobowych i dostępowych.
4. Przechwycenie certyfikatu e-ZLA
Po logowaniu na fałszywej stronie lekarz otrzymuje e-mail o rzekomym unieważnieniu certyfikatu ZUS wraz z linkiem do pobrania „nowego” pliku. Hasłem do niego jest numer PESEL – co wskazuje na próbę wyłudzenia.

5. Zakładanie kont w aplikacjach gabinetowych
Na podstawie skradzionych danych atakujący mogą zakładać konta w niektórych aplikacjach gabinetowych, często nawet bez wiedzy lekarza.
6. Wystawianie recept bez zgody lekarza
Po przejęciu certyfikatu i dostępu do aplikacji gabinetowej przestępcy wystawiają fałszywe recepty na substancje kontrolowane.
Ważne!
Scenariusz może ulegać modyfikacjom.
Jak sprawdzić czy wystawiono recepty bez Twojej wiedzy?

- Wejdź na: gabinet.gov.pl
- Instrukcja: https://ezdrowie.gov.pl/portal/artykul/raport-wystawionych-recept-w-gabinet-gov-pl

Dlaczego kampania jest szczególnie groźna
Cyberprzestępcy:

- wykorzystują strach i presję prawną,
- podszywają się pod instytucje publiczne, co zwiększa ich wiarygodność,
- odwołują się do realnych obaw lekarzy i stosują socjotechnikę.

Przejęcie certyfikatu e-ZLA daje przestępcom realną możliwość wystawiania recept.
Rekomendacje dla lekarzy i podmiotów leczniczych
1. Weryfikuj rozmówcę
Instytucje publiczne nie proszą telefonicznie o logowanie lub podawanie danych. Jeśli masz wątpliwości przerwij rozmowę i oddzwoń na oficjalny numer instytucji.
2. Włącz uwierzytelnianie wieloskładnikowe (MFA)
Aktywuj MFA we wszystkich systemach gabinetowych, poczcie elektronicznej i innych krytycznych usługach.
3. Korzystaj wyłącznie z oficjalnych stron
Nie wchodź w linki ani kody QR przesyłane telefonicznie lub e-mailem przez niezweryfikowane źródła.
4. Regularnie monitoruj wystawione recepty
Cykliczna kontrola konta w gabinet.gov.pl pozwala szybko wykryć nadużycia.
5. Monitoruj swoje dane kontaktowe m.in. w Profilu Zaufanym i aplikacjach gabinetowych
Cyberprzestępcy często posługują się przejętym Profilem Zaufanym. Warto sprawdzić, czy np. adres e-mail oraz pozostałe dane są poprawne i wszystkie informacje trafiają do odpowiedniego odbiorcy. Jest to istotne, ponieważ atakujący często zmieniają dane kontaktowe w aplikacjach gabinetowych oraz w Profilu Zaufanym, aby potencjalne oznaki przejęcia konta nie trafiały do lekarza.
Wskaźniki kompromitacji (IOC)

- Podejrzane domeny
  - eincydent[.]org
  - e-incydent[.]org
  - m-incydent[.]org
-

Nazwiska używane przez oszustów
    - Tomasz Zieliński
    - Tomasz Ochocki
- Adresy e-mail wykorzystywane w kampanii
    - tomaszochocki1@atomicmail.io
    - tomoch12@int.pl
    - tomaszochocki664@int.pl
- Adresy IP fałszywych stron
    - 172.67.143.246
    - 104.21.71.79
- Numery telefonów wykorzystywane w atakach
    - +48 21 223 07 00
    - +420 736 449 192
    - +420 739 443 974

Podsumowanie
Trwająca kampania to jedno z najbardziej zaawansowanych i szkodliwych działań wymierzonych w środowisko lekarskie. Jej celem jest:

- kradzież danych,
- przejecie dostępów do Profilu Zaufanego i aplikacji gabinetowych,
- przejęcie certyfikatów e-ZLA,
- zakładanie nowych kont w aplikacjach gabinetowych z wykorzystaniem wykradzionych danych lekarza,
- wystawianie recept bez uprawnień.

Najważniejszą ochroną jest ostrożność, stosowanie MFA, weryfikacja rozmówców i korzystanie z oficjalnych kanałów.
Przejęcie dostępu do aplikacji gabinetowych skutkuje nie tylko nieuprawnionym wystawianiem recept na leki psychotropowe i narkotyczne, lecz **przede wszystkim uzyskaniem dostępu do wrażliwych danych osobowych pacjentów.** Dane te objęte są szczególną ochroną na gruncie RODO, a naruszenie ich poufności powinno być zgłoszone do Prezesa UODO.
Więcej informacji: Cyberprzestępcy atakują lekarzy! Próby przejęcia tożsamości i wystawiania recept bez autoryzacji | Centrum e-Zdrowia