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 atakach spear phishing na pracowników polskich firm i instytucji publicznych

2023-03-23 14:56:43

Pełna treść ostrzeżenia dostępna w komunikacie "Ataki spear phishing na pracowników polskich firm i instytucji publicznych" na stronie CERT.

- **Szczególnie narażeni użytkownicy: Pracownicy firm i instytucji publicznych**
- **Wektor ataku: Wiadomości e-mail oraz Whatsapp**
- **Możliwe skutki: Kradzież środków finansowych**
- **Atakowane platformy: różne**

Spear phishing jest oszustwem o charakterze socjotechnicznym, wykorzystującym presję autorytetu i czasu, aby skłonić atakowanego do podjęcia niekorzystnego działania. Fakt, że zazwyczaj informacje potrzebne do przeprowadzenia ataku są publicznie dostępne lub łatwe do uzyskania, czyni to oszustwo popularnym wśród cyberprzestępców.

Schemat działania

Najczęstszym wektorem ataku są wiadomości e-mail. Ich treść sugeruje, że zaistniała konieczność natychmiastowej weryfikacji stanu konta lub uaktualnienia danych do przelewu, które w rzeczywistości są numerem konta oszusta. Sprawa może dotyczyć zarówno konta osobistego, jak i konta instytucji, w której pracujemy. Tego typu wiadomości mogą mieć charakter zarówno bardzo ogólnikowy, w postaci niepodpisanego e-maila, jak i być doskonale przygotowaną wiadomością, ze stopką instytucji i podpisem pracownika, najczęściej wysokiego szczebla. Niestety taki rodzaj ataku jest łatwy w przygotowaniu, ponieważ prawie wszystkie potrzebne dane są ogólnodostępne.

Kolejnym wektorem ataku są wiadomość na komunikatorze WhatsApp, gdzie na wstępie atakujący pisząc z obcego numeru, przedstawia się jako rzekomy pracownik i, tłumacząc zmianę numeru awarią czy zgubieniem telefonu, nakłania do podjęcia określonych działań, które mają na celu wyłudzenie pieniędzy.

Ważne informacje

E-maile przy tego typu oszustwach mogą przychodzić zarówno z przypadkowych adresów i domen, jak i takich, które są właściwe dla danego podmiotu. W drugim przypadku przestępcy wykorzystują spoofing, czyli podszycie się pod danego adresata, co jest możliwe dzięki słabościom systemów mailowych, w szczególności z powodu błędów konfiguracyjnych dwóch mechanizmów - SPF i DMARC, o których można przeczytać w naszym artykule.

Skutki oszustwa

Przestępcy w trakcie komunikacji mają zwykle jeden cel - przekonanie nieświadomego pracownika do przelewu pieniędzy na konto oszustów. Warto zauważyć, że jest to zazwyczaj konto zagranicznego banku, co ma utrudnić odzyskanie pieniędzy.

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 zrobić w przypadku zainfekowania komputera szkodliwym oprogramowaniem?

W takim przypadku należy:

- **jak najszybciej skontaktować się z działem bezpieczeństwa w swojej organizacji**
- **zgłosić sprawę do banku, który świadczy usługi firmie albo instytucji**
- **zgłosić sprawę na najbliższym komisariacie Policji**

W razie pytań lub wątpliwości zachęcamy do kontaktu z naszym zespołem. Podejrzane strony oraz oprogramowanie można nam zgłosić za pomocą formularza na stronie Zgłoś incydent CERT.PL lub za pośrednictwem wiadomości e-mail na adres: cert@cert.pl.

Dziękujemy za odwiedziny i zapraszamy ponownie

bezpośredni link do strony www