Ostrzeżenie Cyberbezpieczeństwa

Phishing przez komunikator Signal

Opis zagrożenia

Ujawnione w ostatnim czasie incydenty bezpieczeństwa komputerowego wskazują na **utrzymujące się wysokie zagrożenie** związane z atakami phishingowymi wymierzonych w użytkowników aplikacji Signal. Przedmiotowe ataki przypisywane są aktywnościom adwersarzy działających zgodnie z **interesami Federacji Rosyjskiej**. Wspomniane działania stanowią element szerokiej kampanii phishingowej mającej na celu **przejęcie kont Signal** należących do polityków, urzędników państwowych oraz personelu wojskowego.

Atakujący, po skutecznym przejęciu konta, może uzyskać dostęp do numerów telefonów kontaktów ofiary oraz odczytywać wiadomości otrzymywane przez ofiarę. W określonych sytuacjach, adwersarz może również odczytywać wiadomości w rozmowach grupowych, do których należy ofiara. Należy zaznaczyć, że ataki tego rodzaju nie wykorzystują złośliwego oprogramowania. Atakujący korzystają wyłącznie z wbudowanych funkcji bezpieczeństwa aplikacji w połączeniu z technikami inżynierii społecznej.

Warianty ataku

Występują dwa główne warianty przeprowadzenia ataku.

1. **Przejęcie konta**

   Atakujący podszywają się pod oficjalny zespół wsparcia lub chatbota pomocy technicznej komunikatora. Ofiara otrzymuje wiadomość rzekomo wysłaną przez „Signal Security Support Chatbot", lub „Signal Support”. Treści fałszywych wiadomości wykorzystują motywy informowania użytkowników o zaobserwowaniu:

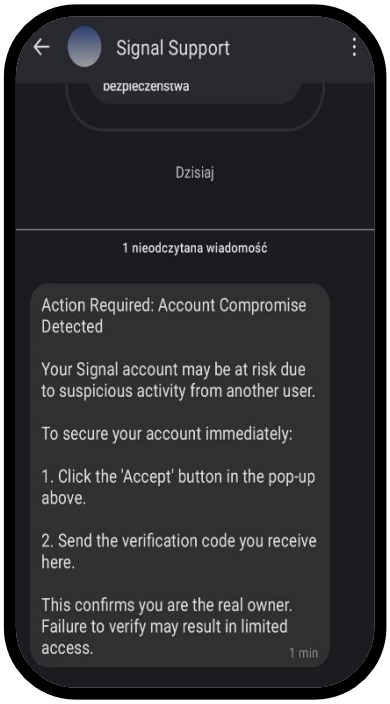
   - podejrzanej aktywności na koncie użytkownika
   - włamania się na konto i kradzieży danych użytkownika
   - prób nieautoryzowanego logowania się na konto użytkownika

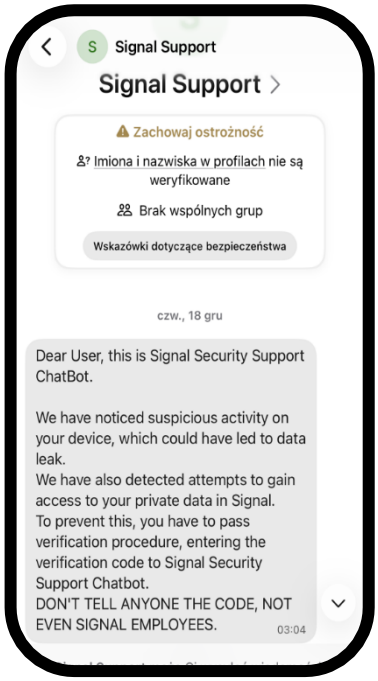
   Następnie atakujący próbuje wyłudzić od użytkownika, kod weryfikacyjny SMS i PIN do aplikacji, stosując manipulację sugerującą, że w ten sposób ofiara może zapobiec atakowi. W rzeczywistości, wykorzystując te kody, atakujący przejmuje pełną kontrolę nad kontem użytkownika, a ofiara traci do niego dostęp.

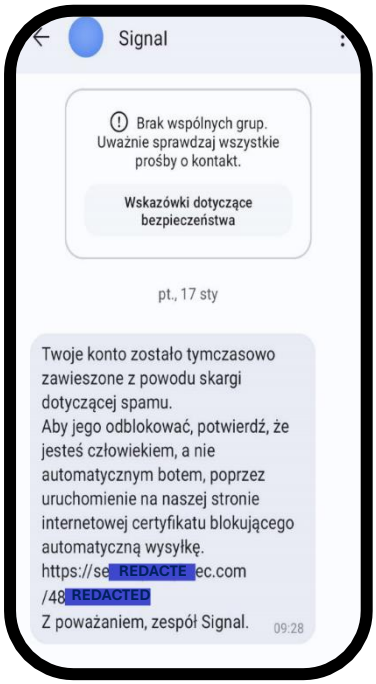
2. Powiązanie urządzenia

Atakujący wykorzystują techniki inżynierii społecznej, aby skłonić ofiarę do zeskanowania kodu QR lub uruchomienia odnośnika (link). Linki i kody QR mogą służyć do dodawania kontaktów, osób do grup oraz powiązywania aplikacji z innym urządzeniem. Atakujący może wysłać ofierze kod QR lub link rzekomo zapraszający ją do grupy, podczas gdy w rzeczywistości wykonanie tej czynności powiąże urządzenie atakującego z kontem ofiary. Prowadzi to do przekazania atakującemu pełnego dostępu do wszystkich czatów ofiary, najczęściej wraz z historią rozmów. Atakujący może również odczytywać i wysyłać wiadomości w jej imieniu. Ofiara zachowuje dostęp do swojego konta, ale zazwyczaj nie dostrzega od razu, że ktoś inny ma wgląd do jej komunikacji.

Przykłady złośliwych wiadomości znajdują się poniżej:







Zalecenia i rekomendacje

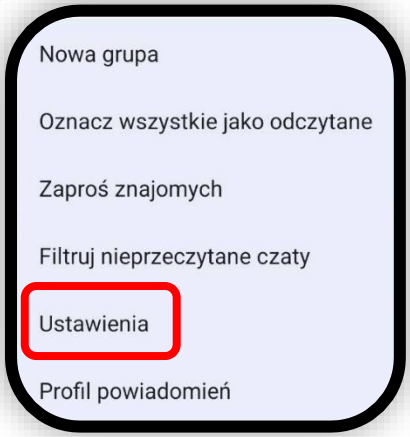
Niezależnie od stosowanych zabezpieczeń, zawsze istnieje ryzyko utraty danych. Korzystaj z komunikatorów rozsądnie. Uważaj z kim utrzymujesz kontakt i jakie informacje przekazujesz. Nigdy nie używaj komunikatora do przesyłania informacji niejawnych ani wrażliwych.

- Regularnie sprawdzaj listę urządzeń, które mają dostęp do Twojego konta Signal. Niezwłocznie usuwaj urządzenia, których nie rozpoznajesz.
- Dział obsługi klienta aplikacji Signal nigdy nie kontaktuje się z użytkownikami bezpośrednio poprzez wiadomości w komunikatorze.
- Blokuj lub zgłaszaj konta podszywające się pod wsparcie techniczne aplikacji Signal.
- Nigdy nie podawaj swojego PIN-u i kodu SMS w wiadomości Signal.
- Skanuj kody QR wyłącznie aplikacją Signal i tylko wtedy, gdy osobiście powiązujesz urządzenie z aplikacją.
- Posługuj się nazwą użytkownika zamiast numerem telefonu i skorzystaj z opcji ukrycia własnego numeru telefonu. Ukrycie numeru telefonu przed atakującym utrudnia ataki phishingowe oraz przejęcie konta.
- Aktywuj funkcję „Blokada rejestracji”

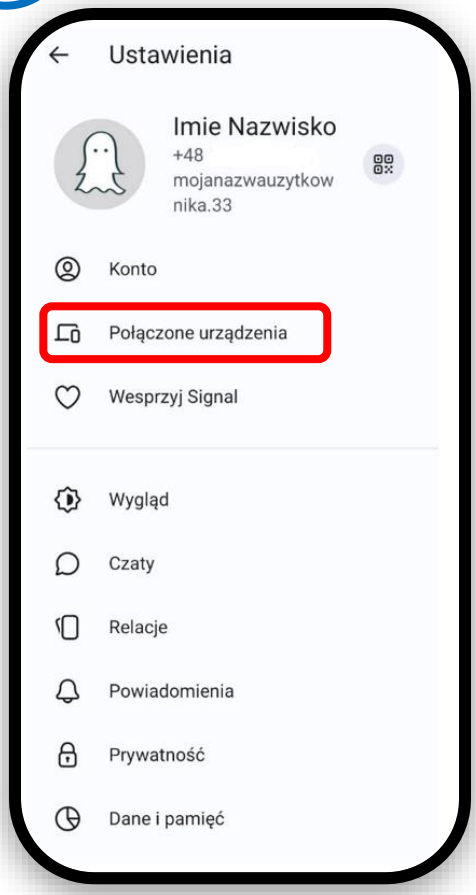
Rekomendacje w zakresie weryfikacji aktualnie podłączonych urządzeń do konta Signal.

1

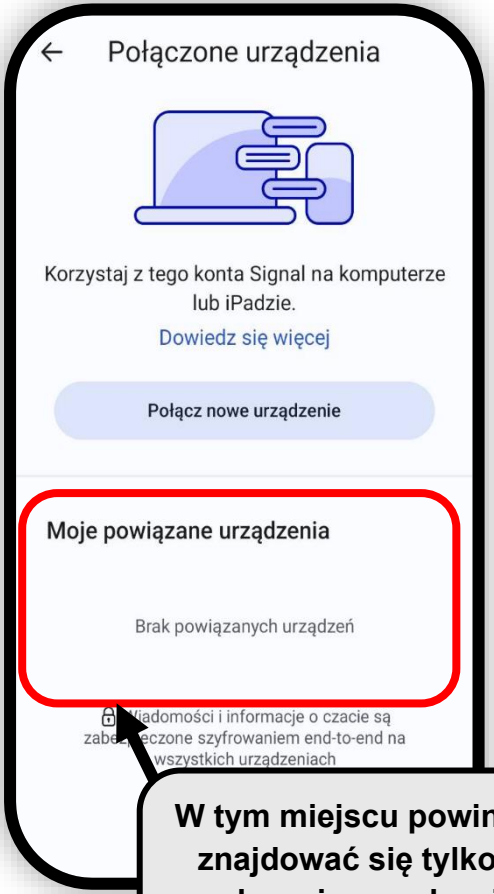
2



3



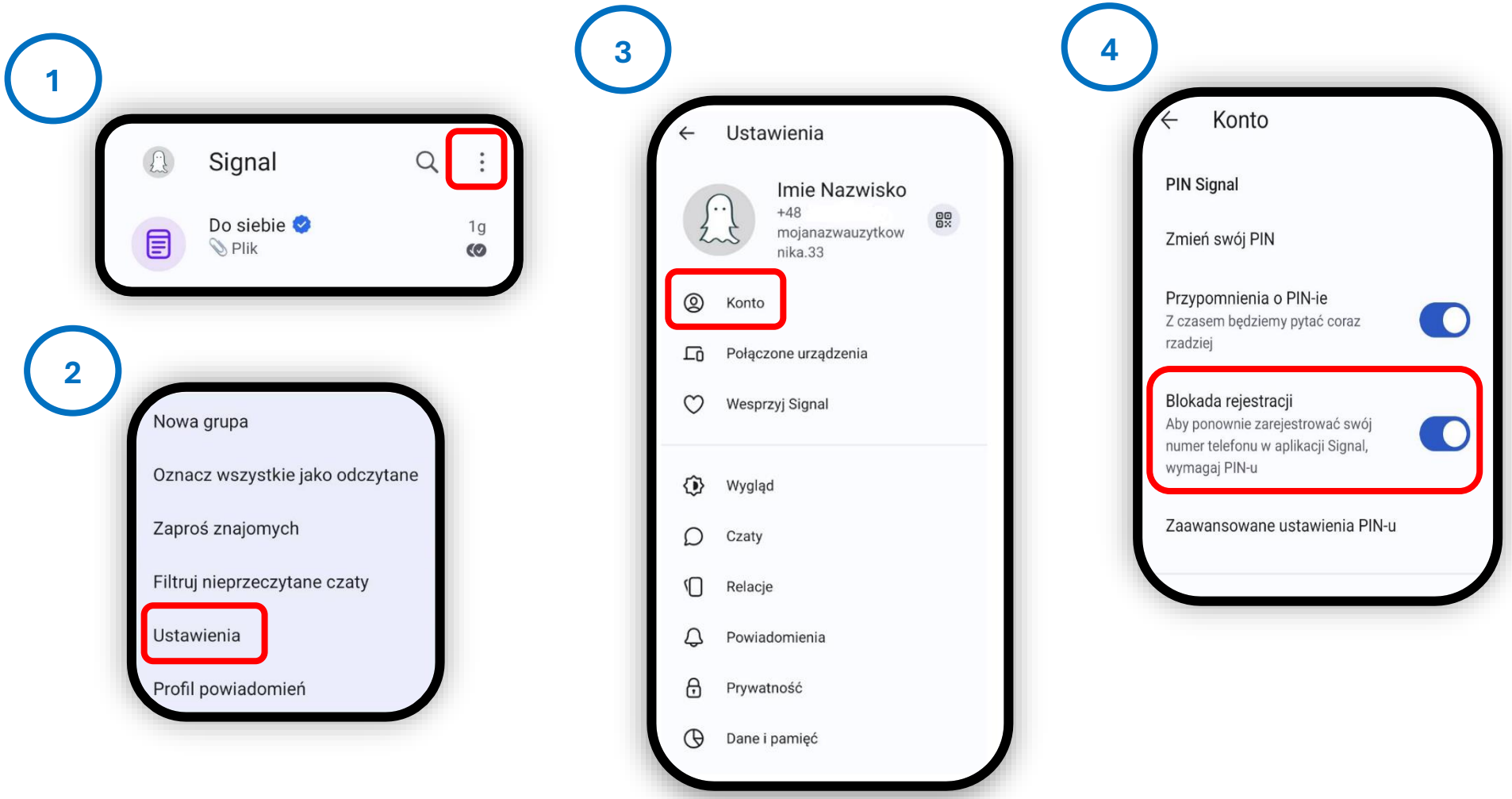
4



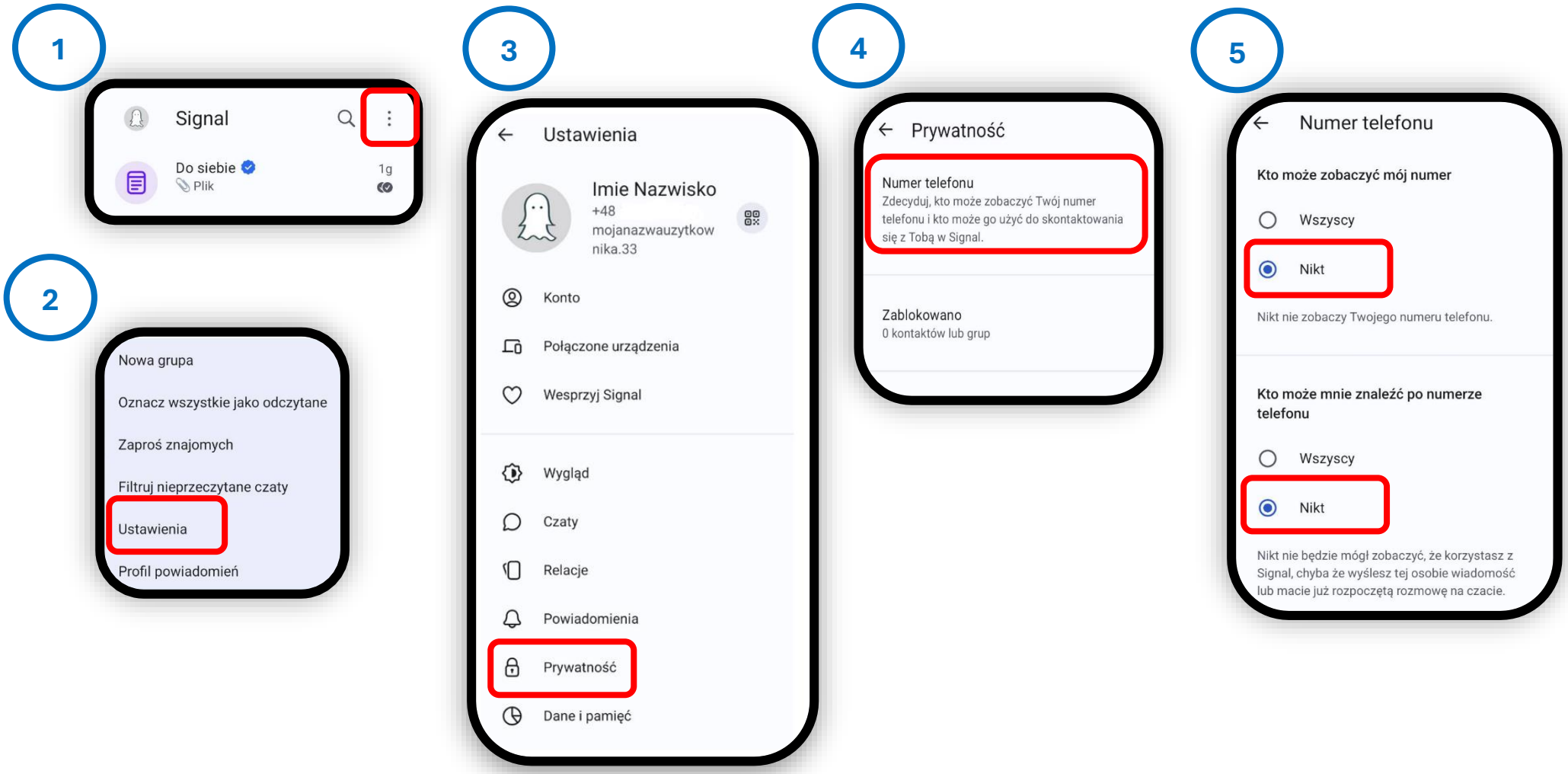
W tym miejscu powinny znajdować się tylko i wyłącznie urządzenia właściciela konta

Rekomendacje w zakresie bezpiecznej konfiguracji komunikatora Signal.

1. Uruchomienie opcji „Blokada rejestracji”, celem wdrożenia dodatkowego składnika autoryzacyjnego w momencie podłączania kolejnego urządzenia do konta Signal. Opcja ta chroni przed nieuprawnionym podłączeniem dodatkowego urządzenia nawet w przypadku wyłudzenia kodu autoryzacyjnego przesłanego przez SMS.



2. Uruchomienie ustawień prywatności w zakresie widoczności numer telefonu powiązanego z kontem Signal. Uwaga! Wprowadzenie tej konfiguracji sprawi, że wyszukanie użytkownika za pomocą numeru telefonu będzie niemożliwe. Od tego momentu konto może zostać wyszukane za pomocą unikalnej nazwy użytkownika widocznego tylko dla właściciela konta.



3. Ustawienie unikalnej nazwy użytkownika swojego konta po ukryciu numeru telefonu w aplikacji Signal.