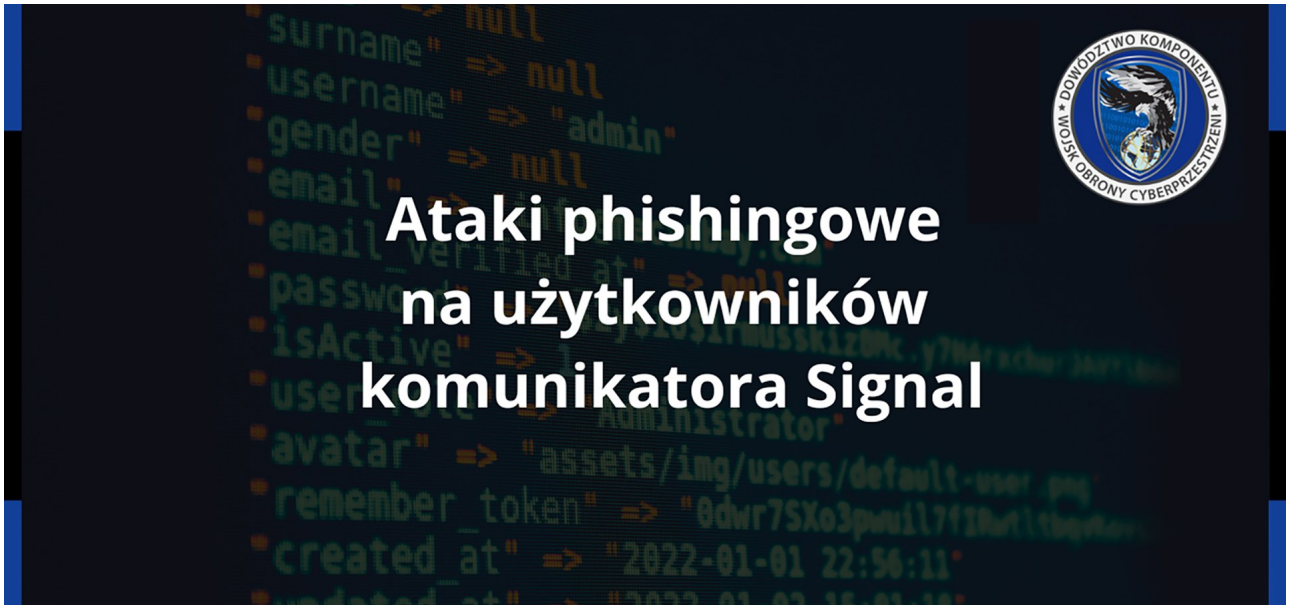
05 czerwca 2025

Ataki phishingowe wymierzone w użytkowników komunikatora Signal



Na urządzenia użytkowników komunikatora Signal trafiają coraz częściej wiadomości rzekomo wysłane przez konta identyfikujące się jako „Signal Support", „Signal Notification" lub „Zespół Signal". Fałszywi nadawcy alarmują o „naruszeniu bezpieczeństwa konta" i nakłaniają odbiorców do podania sześciocyfrowego kodu przesłanego przez SMS. Kod ten to klucz do przejęcia konwersacji i dodania urządzenia atakującego do konta ofiary.

Kod, który otwiera drzwi do prywatności

Aplikacja Signal stosuje szyfrowanie typu end-to-end – każdy klucz prywatny znajduje się wyłącznie na urządzeniu użytkownika. Atakujący, chcąc czytać wiadomości, próbują uzyskać dostęp do samego urządzenia lub konta Signal ofiary.

Rejestracja i każdorazowe dodanie nowego urządzenia opierają się na numerze telefonu oraz jednorazowym sześciocyfrowym kodzie wysłanym SMS-em. Atakujący zdobywając ten kod, może dodać własny telefon lub komputer jako kolejne urządzenie i dyskretnie czytać całą korespondencję w czasie rzeczywistym. Nie trzeba infekować urządzenia ofiary ani znać jej hasła.

Sześciocyfrowy kod instalacyjny, wysyłany poprzez SMS, umożliwia logowanie na nowym urządzeniu. Przekazując go osobie trzeciej, praktycznie zapraszamy ją do wszystkich naszych konwersacji. Po udanym ataku ofiara nie widzi, że ktoś skrycie czyta korespondencję, bo wszystkie wiadomości nadal docierają na jej telefon.

Atak – krok po kroku

1. Fałszywy alert – wiadomość przychodzi bez poprzedzającego zgłoszenia, często późnym wieczorem, prawdopodobnie by wywołać pośpiech u potencjalnej ofiary.

2. Groźba blokady – nadawca wiadomości straszy zamknięciem konta z powodu nieokreślonego „naruszenia".

3. Prośba o kod – „dla potwierdzenia tożsamości” trzeba odesłać kod SMS lub uruchomić link prowadzący do fałszywej strony logowania.

Podszywanie się pod „Signal Support” działa psychologicznie

Komunikat pojawia się w oknie aplikacji, więc odruchowo wzbudza większe zaufanie niż SMS czy e-mail. Fałszywe alerty wykorzystują niepokój („Twoje konto zostanie zablokowane”) i autorytet rzekomego zespołu wsparcia. Użytkownicy są przyzwyczajeni, że kody SMS często wykorzystywane są w procedurach bezpieczeństwa; proszenie o nie przez „support” nie wydaje się nienaturalne, zwłaszcza przy braku technicznego kontekstu.

Aplikacja Signal nigdy nie prosi o taki kod

W przypadku otrzymania podejrzanej wiadomości należy nacisnąć przycisk „Zgłoś”, a następnie „Zablokuj”. DKWOC rekomenduje wdrożenie bezpiecznej konfiguracji komunikatora Signal oraz weryfikację aktualnie podłączonych urządzeń zgodnie z instrukcją załączoną do niniejszej publikacji. Jeżeli kod został już przekazany, należy niezwłocznie wylogować wszystkie sesje („Wyloguj wszystkie urządzenia”), ponownie zarejestrować numer i skonfigurować aplikację zgodnie z załączonymi rekomendacjami.

Multi-device w Signal zwiększa powierzchnię ataku

Od czasu wprowadzenia oficjalnej obsługi wielu urządzeń (telefon + kilka desktopów/tabletów) do konta można, bez odłączania bieżącego telefonu, dodać nowe urządzenia. Jeśli ofiara nie sprawdzi ustawień zakładki „Podłączone urządzenia” w folderze “Ustawienia” aplikacji Signal, nie zauważy cichego podsłuchu.

Nie tylko Signal

Komunikatory powiązane z numerem telefonu, takie jak Signal czy WhatsApp, to naturalny cel ataku. Ten sam scenariusz może więc spotkać użytkowników innych aplikacji. Signal stanowi atrakcyjny cel z uwagi na gromadzenie wrażliwych rozmów, zdjęć i plików, a „klucz” do konta – kod SMS – da się zdobyć metodą socjotechniczną. Im silniejsze jest zabezpieczenie kryptograficzne samej platformy, tym częściej atakujący wykorzystują słabości użytkownika a nie algorytmy.

Rekomendacje w zakresie weryfikacji aktualnie podłączonych urządzeń do konta Signal oraz rekomendacje w zakresie bezpiecznej konfiguracji komunikatora Signal znajdują się w załączniku poniżej.