Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

KOMUNIKAT

w sprawie kampanii wymierzonej w użytkowników komunikatora Signal

Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego obserwują kampanie phishingowe wymierzone w użytkowników komunikatora Signal. Za działaniami tymi stoi zaawansowana technicznie grupa typu APT, która może być powiązana ze służbami wrogo nastawionych do Polski państw. Obserwacja aktywności grupy wskazuje, że jej działania są przede wszystkim ukierunkowane na osoby zajmujące eksponowane stanowiska publiczne lub rozpoznawalne ze względu na swoją działalność polityczną (w tym ministrowie, parlamentarzyści, samorządowcy).

Sprawcy wysyłają spreparowane wiadomości, w których w jednym z wariantów podszywają się pod obsługę komunikatora Signal i informują o rzekomym zablokowaniu konta. Następnie w wiadomości znajduje się instrukcja, według której odblokowanie konta możliwe jest po odwiedzeniu wskazanej strony internetowej.

Przykładowa treść wiadomości wykorzystywanej w kampanii:

Należy mieć na uwadze, że wiadomości mają wiele wariantów i mogą różnić się od przykładowej. W przypadku otrzymania takiej lub podobnej wiadomości, w szczególności kiedy zawiera link i budzi podejrzenia, należy:

1. **Nie otwierać linku znajdującego się w wiadomości.**
2. Nie blokować kontaktu, z którego przyszła wiadomość.

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres:
ul. Królewska 27
00-060 Warszawa

3a. W przypadku urządzeń prywatnych: dokonać zgłoszenia incydentu do CSIRT NASK: https://incydent.cert.pl.

3b. W przypadku urządzeń służbowych: dokonać zgłoszenia incydentu do komórki odpowiedzialnej za cyberbezpieczeństwo w ramach organizacji, a ta powinno zgłosić incydent do właściwego CSIRT.

Zastosowanie się do powyższych zaleceń pozwoli ustrzec się przed przejęciem konta.

W przypadku kliknięcia w link lub wykonania dalszych kroków, należy pilnie zgłosić incydent do CSIRT NASK (w przypadku urządzeń prywatnych) lub do komórki odpowiedzialnej za cyberbezpieczeństwo w organizacji (w przypadku urządzeń służbowych). Docelowo kampania ta może prowadzić do utraty poufności korespondencji prowadzonej z wykorzystaniem komunikatora Signal. Atakujący uzyskują stały dostęp do wiadomości ofiary.

Niezależne od powyższego zalecane jest takie skonfigurowanie ustawień komunikatora Signal, które podniesienie poziom prywatności i bezpieczeństwa wykorzystywania tej aplikacji, takie jak numer bezpieczeństwa[1]. W przypadku innych komunikatorów zalecane jest wprowadzenie analogicznych ustawień, o ile są dostępne w danym rozwiązaniu.

Jednocześnie Ministerstwo Cyfryzacji przypomina, że na potrzeby administracji publicznej udostępnia bezpieczny Komunikator na urządzenia służbowe (gdzie podobny atak phishingowy nie jest możliwy z uwagi architekturę rozwiązania), jak również mobilny system łączności niejawnej SKR-Z (gdzie również tego typu atak nie jest możliwy).

Ministerstwo Cyfryzacji zachęca podmioty Krajowego Systemu Cyberbezpieczeństwa do korzystania z bezpłatnych szkoleń[2], których tematyka obejmuje również przeciwdziałanie tego rodzaju zagrożeniom.

Ponadto, Ministerstwo Cyfryzacji we współpracy z NASK-PIB w ramach projektu SecureV prowadzi specjalistyczne, indywidualne szkolenia z zakresu cyberbezpieczeństwa dla osób pełniących kierownicze funkcje w administracji publicznej, które także obejmują kwestie higieny cyfrowej i ochrony przed phishingiem. Osoby pełniące tego rodzaje funkcje, w tym parlamentarzystów oraz kierownictwo ministerstw i urzędów centralnych, zachęcamy do kontaktu z Departamentem Cyberbezpieczeństwa Ministerstwa Cyfryzacji, aby pozyskać szczegółowe informacje o możliwości skorzystania ze szkoleń SecureV.

Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

---

[1] https://support.signal.org/hc/pl/articles/6712070553754-Prywatno%C5%9B%C4%87-numery-telefonu-a-nazwa-u%C5%BCytkownika

[2] https://www.gov.pl/web/baza-wiedzy/harmonogramszkolen