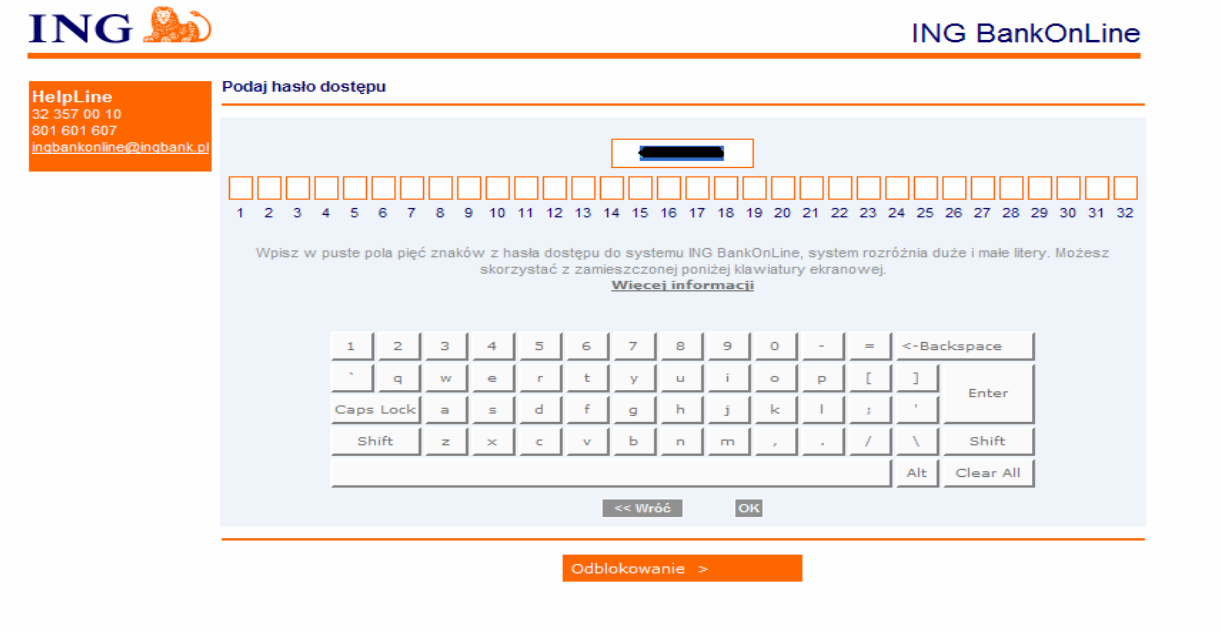
Wstęp

W Internecie ukazała się informacja o nowej wersji Trojana Zeus/Zbot, w której wprowadzono mechanizm pozwalający na wykonanie ataku na Klientów bankowości internetowej, którzy korzystają z kodów do autoryzacji transakcji przesyłanych SMS-em.
Atak został nazwany Man-in-the-Mobile.

Opis

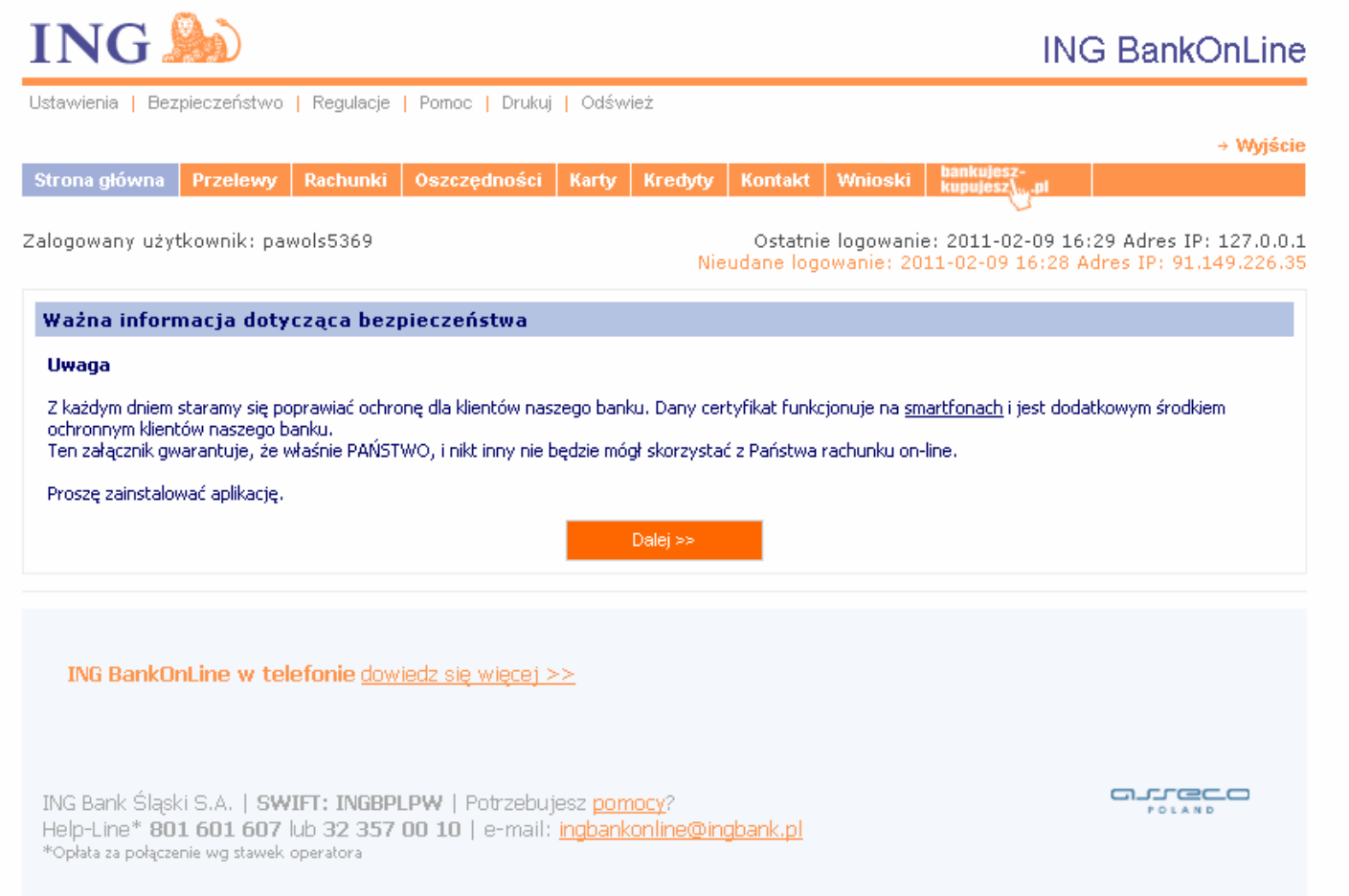
Trojan korzysta z istniejącego już mechanizmu pozyskania użytkownika i hasła do bankowości internetowej. (rys.1)

Bank nigdy nie prosi Klienta o podanie PEŁNEGO HASŁA dostępu do usługi ING Bank OnLine.



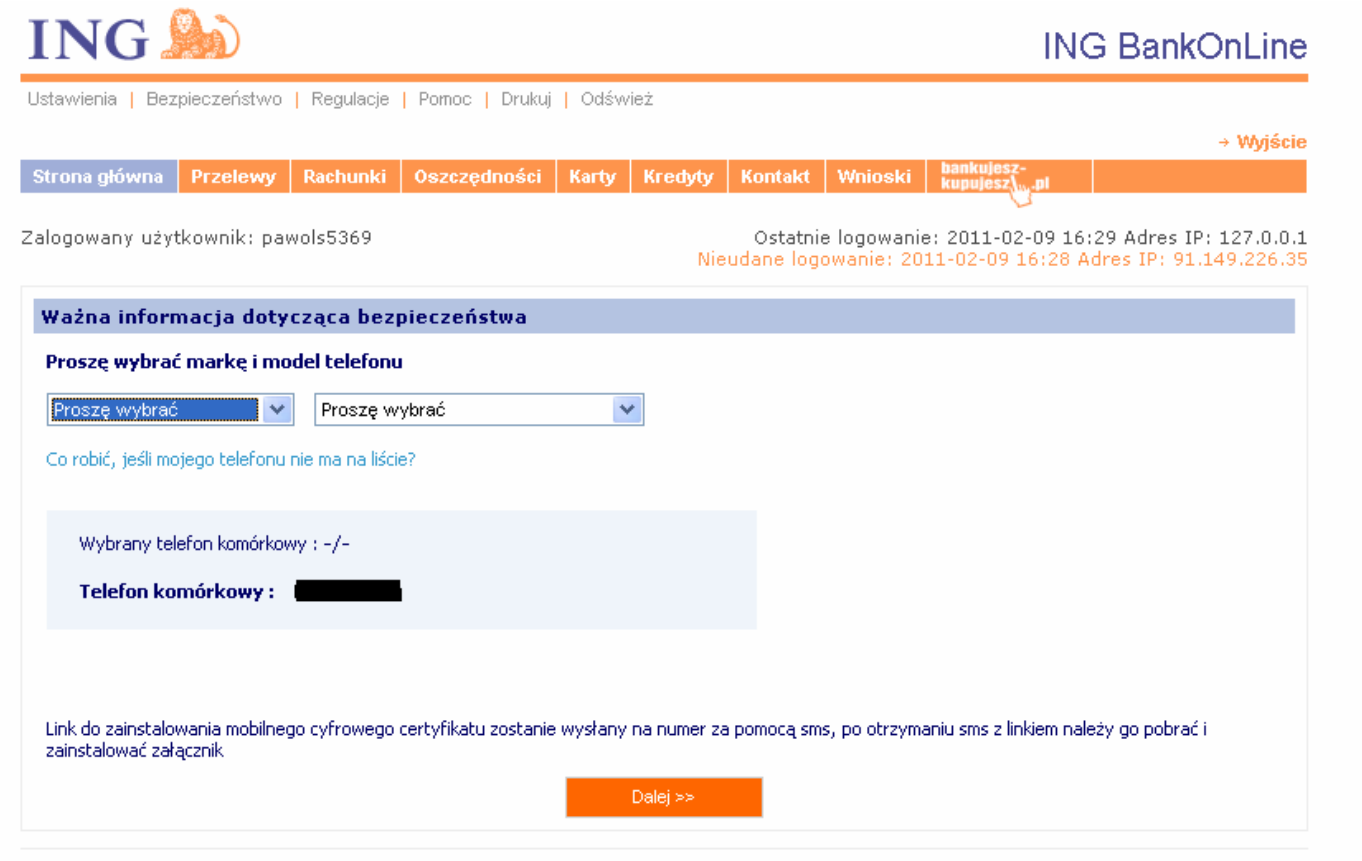
Rysunek 1. Prośba o podanie pełnego hasła

Atak ten został uzupełniony o działania socjotechniczne wykorzystujące Man-in-the-Browser (MitB). (rys2)



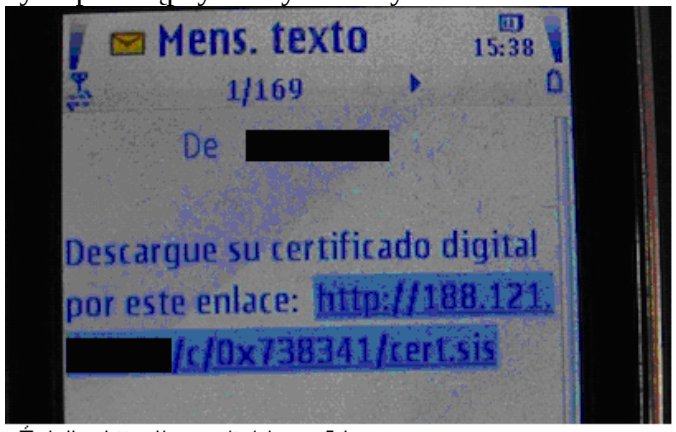
Rysunek 2.

Atak MitB ma na celu pozyskanie informacji o telefonie Klienta wykorzystywanym do kodów SMS takich jak producent, model i numer telefonu. Prośba o podanie tych danych jest tłumaczona wprowadzeniem nowych środków bezpieczeństwa (**Rysunek 3)**.



Rysunek 3. Przykładowy atak Trojana Zeus/Zbot mający na celu pozyskanie informacji o telefonie Klienta

Klient po podaniu danych otrzymuje SMS'a (**Rysunek 4)** z linkiem do pobrania nowego certyfikatu bezpieczeństwa, który w rzeczywistości jest złośliwą aplikacją. Aplikacja ta monitoruje przychodzące SMS'y i uruchamia tylne wejście (backdoor) pozwalające na zarządzanie telefonem Klienta, poprzez SMS'y cyberprzestępcy. Głównym zadaniem aplikacji jest przesyłanie SMS'ów przychodzących z banku na numer telefonu cyberprzestępcy i ukrywanie tych działań.



Źródło: http://securityblog.s21sec.com

Rysunek 4. Przykładowy SMS z linkiem

Co możemy zrobić by ograniczyć możliwość wystąpienia opisanego powyżej ataku?

Po pierwsze ING Bank Śląski nie prosi Klientów o podawanie informacji na temat używanego do autoryzacji telefonu oraz nie wymaga instalacji żadnego oprogramowania na tychże telefonach, aby autoryzować transakcje za pomocą kodów SMS.

Po drugie należy zabezpieczyć komputer:

- Zainstaluj niezbędne programy zabezpieczające tj program antywirusowy czy zaporę ogniową
- Regularnie aktualizuj system operacyjny Windows i sygnatury antywirusowe
- Zabezpiecz komórkę instalując program antywirusowy

Po trzecie nie należy:

- Otwierać podejrzanych maili lub SMS-ów oraz korzystać z podawanych tam linków czy załączników
- Instalować oprogramowania nieznanego pochodzenia
- Odwiedzać podejrzanych stron WWW

Po czwarte zachowaj zdrowy rozsądek, traktuj z dystansem wszystkie maile, SMS'y i telefony, w których jesteś proszony o dane osobowe, PIN czy hasło. Jeżeli nawet na stronie banku zostałeś poproszony o podanie danych, o które do tej pory bank nie pytał, zadzwoń do banku i sprawdź czy na pewno o te dane pyta bank a nie Trojan Zeus!

Chcesz wiedzieć więcej? Przeczytaj o bezpieczeństwie na stronie ING Banku Śląskiego.