

## 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.



The screenshot shows the ING Bank OnLine login interface. At the top left is the ING logo and a HelpLine contact box. The main heading is "Podaj hasło dostępu". Below it is a password input field containing a masked password. Underneath the field is a row of 32 numbered boxes (1-32) for entering the password. A text instruction reads: "Wpisz w puste pola pięć znaków z hasła dostępu do systemu ING BankOnLine, system rozróżnia duże i małe litery. Możesz skorzystać z zamieszczonej poniżej klawiatury ekranowej." Below this is a link for "Wiecej informacji". A numeric keypad is displayed with buttons for digits 1-0, hyphen/underscore, equals, backspace, and function keys like Caps Lock, Shift, Alt, and Clear All. At the bottom of the keypad are buttons for "<< Wróć" and "OK". Below the keypad is an orange button labeled "Odblokowanie >".

Rysunek 1. Prośba o podanie pełnego hasła

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



**ING**  **ING BankOnLine**

Ustawienia | Bezpieczeństwo | Regulacje | Pomoc | Drukuj | Odśwież

[Strona główna](#) | [Przelewy](#) | [Rachunki](#) | [Oszczędności](#) | [Karty](#) | [Kredyty](#) | [Kontakt](#) | [Wnioski](#) | [bankujesz-kupujesz.pl](#) [→ Wyjście](#)

Zalogowany użytkownik: pawols5369 Ostatnie logowanie: 2011-02-09 16:29 Adres IP: 127.0.0.1  
Nieudane logowanie: 2011-02-09 16:28 Adres IP: 91.149.226.35

**Ważna informacja dotycząca bezpieczeństwa**

**Uwaga**

Z każdym dniem staramy się poprawiać ochronę dla klientów naszego banku. Dany certyfikat funkcjonuje na [smartfonach](#) i jest dodatkowym środkiem ochronnym klientów naszego banku. Ten załącznik gwarantuje, że właśnie PAŃSTWO, i nikt inny nie będzie mógł skorzystać z Państwa rachunku on-line.

Proszę zainstalować aplikację.

[Dalej >>](#)

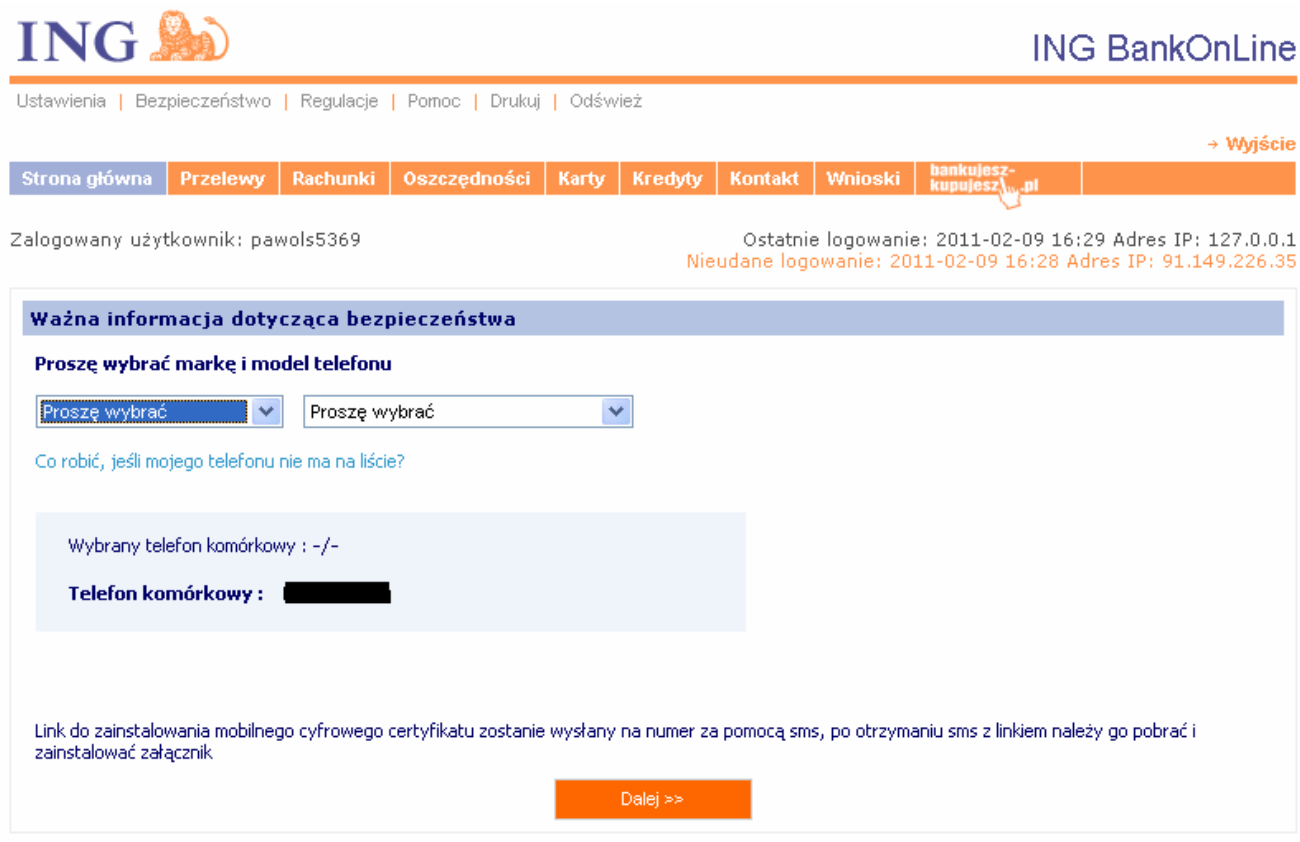
[ING BankOnLine w telefonie dowiedz się więcej >>](#)

ING Bank Śląski S.A. | SWIFT: INGBPLPW | Potrzebujesz [pomocy?](#)  
Help-Line\* 801 601 607 lub 32 357 00 10 | e-mail: [ingbankonline@ingbank.pl](mailto:ingbankonline@ingbank.pl)  
\*Opłata za połączenie wg stawek operatora



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**).



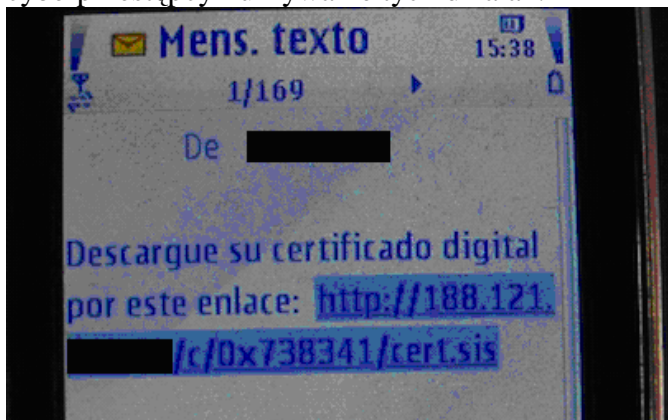
The screenshot shows the ING BankOnline interface. At the top left is the ING logo, and at the top right is the text "ING BankOnLine". Below the logo is a navigation bar with links: "Ustawienia", "Bezpieczeństwo", "Regulacje", "Pomoc", "Drukuj", "Odśwież". To the right of this bar is a "Wyjście" link. Below the navigation bar is a menu with buttons for "Strona główna", "Przelewy", "Rachunki", "Oszczędności", "Karty", "Kredyty", "Kontakt", "Wnioski", and "bankujesz-kupujesz.pl".

Below the menu, the user is logged in as "pawols5369". The last login was on 2011-02-09 at 16:29 from IP 127.0.0.1. A failed login attempt was on 2011-02-09 at 16:28 from IP 91.149.226.35.

The main content area features a blue header with the text "Ważna informacja dotycząca bezpieczeństwa". Below this, the user is prompted to "Proszę wybrać markę i model telefonu". There are two dropdown menus, both currently showing "Proszę wybrać". A link "Co robić, jeśli mojego telefonu nie ma na liście?" is provided. Below the dropdowns, a light blue box displays "Wybrany telefon komórkowy : -/-" and "Telefon komórkowy : [REDACTED]". At the bottom of the box, there is a note: "Link do zainstalowania mobilnego cyfrowego certyfikatu zostanie wysłany na numer za pomocą sms, po otrzymaniu sms z linkiem należy go pobrać i zainstalować załącznik". A "Dalej >>" button is located at the bottom right of the box.

**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](#).**

*Prezentowane informacje oparte są na faktach opisanych w ogólnie-dostępnych publikacjach i służą jedynie poszerzeniu wiedzy ich czytelników o zagrożeniach występujących w Internecie.*