Malweare TINBA i VAWTRAK

Szanowni Państwo, informujemy o pojawieniu się ostrzeżenia Związku Banków Polskich o nowym zagrożeniu.

Jest to metoda na tzw. „poczekalnię". Działanie tego złośliwego oprogramowania polega na dodaniu skryptu, który podczas logowania do sesji bankowości internetowej wykonuje następujące czynności:

- Klient podaje hasło i login do bankowości internetowej, które są następnie przesyłane na serwer hakerów,
- Na komputerze klienta przez okres czasu około minuty lub dłużej wyświetlany jest komunikat „ trwa przesyłanie danych" , „proszę czekać", „trwa aktualizacja danych" itp.;

W tym czasie na podstawie wykradzionego loginu i hasła następuje:

- logowanie przez hakerów do bankowości internetowej klienta,
- badanie dostępnych środków,
- przygotowywanie transakcji oszukańczej,
- pobranie informacji z banku o konieczności podania hasła SMS w celu autoryzacji ww. transakcji,

Po tych czynnościach na komputerze nieświadomego klienta skrypt wyświetla komunikat o rzekomych problemach z uwierzytelnieniem i generuje prośbę o wprowadzenie dodatkowego hasła sms w celu prawidłowego przeprowadzenia procesu uwierzytelnienia tożsamości klienta;

Nieświadomy użytkownik wprowadzając hasło sms „de facto" autoryzuje transakcję oszukańczą myśląc, iż dokonuje dodatkowego uwierzytelnienia swojej tożsamości;

W celu opóźnienia identyfikacji kradzieży po wykonaniu przelewu, na zainfekowanym komputerze wyświetlany jest przez trojan komunikat przez hakerów o rzekomych pracach modernizacyjnych i przymusowej przerwie w pracy bankowości internetowej.

```
10  var fkdiv='<tr> <td id="identifier" style="font-weight:bold" align="right" width="135"> <span
    id="login_type_label">Token</span></td><td id="passwordInput" align="left" width="130"><input
    autocomplete="OFF" id="fkresult" size="50" value="" class="short_login_input" style="font-family:tahoma,
    arial, helvetica, sans-serif;" type="password"></td><td> </td></tr>';
11  var waitlok="<div><center> <br/> Prowadzone sa prace modernizacyjne w celu jak najszybszego przywrocenia
    dzialania systemu.<br/>Przyblizony czas modernizacji wynosi kilka godzin.<br/>Przepraszamy za tymczasowe
    utrudnienie i niedogodnosci.<br/><center></div>";
12
```

Ponadto dzięki takim malware'om przestępcy mogą utworzyć nowy przelew zdefiniowany i posiadając już hasło i login do systemu transakcyjnego klienta, mogą samodzielnie dokonywać transakcji oszukańczych z użyciem utworzonego przez siebie przelewu zdefiniowanego (takie przelewy nie wymagają dodatkowej autoryzacji). W związku z powyższym w przypadku gdy użytkownik bankowości internetowej dostrzeże nietypowe działanie systemu bankowości internetowej m. in. wyżej opisane powinien:

- nie podawać dodatkowych informacji w celu „uwierzytelnienia" swojej tożsamości,
- bezzwłocznie skontaktować się ze swoim bankiem w celu powiadomienia banku o odbiegającym do typowego działaniu bankowego serwisu transakcyjnego,
- zmienić hasło dostępowe do systemu bankowości elektronicznej poprzez kanał telefoniczny lub z użyciem innego komputera.

Dobrze byłoby gdyby użytkownik podczas dostrzeżenia ww. anomalii zrobił zrzut ekranu (wciskając przycisk na klawiaturze „PrtScn” i wklejając go do nowego pliku w programie np. „Paint”). Zrzut ten może być pomocny bankowi przy identyfikacji zagrożenia.