CO TO JEST SKIMMING?

Rozwój technologiczny elektronicznych instrumentów płatniczych w tym karty płatniczej, pociągnął za sobą wykształcenie i rozwój nowej formy przestępczości. "Skimming"– ta dla niektórych obco brzmiąca nazwa- jest już znany polskiej Policji. Nie ma tygodnia, by policjanci nie zatrzymali przestępców trudniących się tym procederem. Problem dosyć młody, który na świecie pojawił się w latach 80–tych w Polsce - z wiadomych przyczyn - dopiero pod koniec lat 90-tych minionego wieku.

Mimo swojego "młodego wieku" jest to zjawisko, za którym prawo i w konsekwencji praktyka organów ścigania, w szczególności Policji, próbuje nadążyć i wykształcić swoje mechanizmy obronne. Chodzi przede wszystkim o: zasady postępowania, metody wykrywcze czy w końcu czynności dowodowe.

Poniżej przedstawione zostały rodzaje podziałów występujące przy podziale funkcjonalnym.

Według kryterium funkcji, jakie spełnia karta można wyodrębnić:
- Karty bankomatowe
- Karty płatnicze
- Karty identyfikacyjne
- Karty wstępnie opłacone
- Karty wirtualne

Ze względu na sposób rozliczenia transakcji przy użyciu karty można wyróżnić:
- Karty debetowe
- Karty kredytowe
- Karty z odroczonym terminem płatności i karty obciążeniowe

Najpopularniejsze i najważniejsze przestępstwa z segmentu bankowości elektronicznej to: "skimming", "phishing" i fałszowanie kart płatniczych.

Dzisiaj słów kilka o "skimming-u":

"Skimming" jest terminem zaczerpniętym z języka angielskiego i odnosi się do przestępczego wykorzystania kart płatniczych. Przestępstwo to polega na bezprawnym

skopiowaniu zawartości paska magnetycznego karty bankowej (bankomatowej, kredytowej, itp.) w celu wytworzenia duplikatu oryginalnej karty, która w środowisku elektronicznym zachowywać się będzie identycznie jak karta oryginalna. Transakcje dokonane przy użyciu kopii kart obciążają prawowitego posiadacza karty, niejednokrotnie przy jego nieświadomości. W ostatnim czasie, czego przykładem jest również Polska, "skimming" należy do najgroźniejszych przestępstw związanych z wykorzystaniem kart płatniczych.

Przy pomocy powszechnie dostępnych urządzeń można skopiować całą zawartość paska i zapisać ją na innej karcie. Karty mogą być kopiowane w sklepach, restauracjach, na stacjach benzynowych, w zasadzie w każdym punkcie gdzie można dokonywać płatności kartami. Nieuczciwy sprzedawca może skopiować pasek karty na zapleczu, pod ladą, a nawet na oczach nieświadomego klienta.

Szczególnie groźną odmianą „skimmingu" jest "skimming bankomatowy". W tym przypadku przestępcy instalują specjalistyczne urządzenia, służące do pozyskiwania danych paska magnetycznego kart oraz kodów PIN. Urządzenia mogą być montowane zarówno na bankomatach, jak i w ich wnętrzu.

Przykłady sposobów kopiowania kart płatniczych

Aby wejść w posiadanie danych kart płatniczych, przestępcy wykorzystują w tym celu różne sposoby i urządzenia specjalistyczne. Warto w tym miejscu przedstawić przykłady pozyskiwania danych przy "skimmingu":

• wykorzystanie "skimmerów" oraz mikrokamer lub fałszywych bankomatowych klawiatur przy transakcjach autoryzowanych (sprawcy uzyskują kody PIN kart),

• wykorzystanie "skimmerów" do uzyskania danych z karty (kieszonkowcy, włamywacze, w pokojach hotelowych),

• wykorzystanie chipów umieszczonych w oryginalnych terminalach POS (czasem dodatkowy sprzęt do uzyskania kodów PIN kart),

• włamania crackerów do serwerów sklepów internetowych z danymi kart kredytów klientów tych sklepów,

• podłączanie się do sieci celem uzyskania danych (ang. tapping),

• wykorzystanie podmiotów posiadających i gromadzących dane kart płatniczych (akceptanci, banki, centra personalizacyjne kart płatniczych).

Obecna technika pozwala na tworzenie skanerów tak małych, że w całości mogą zmieścić się w dłoni. Takie urządzenie może służyć do skanowania karty nawet na oczach nieświadomej niczego ofiary.

Skimming w bankomatach to bardziej zaawansowana forma tego procederu, i jak już wspomniano coraz częściej występująca w Polsce. Niezależnie od typu bankomatu oraz zabezpieczeń na nim stosowanych, grupy przestępcze są w stanie zmanipulować bankomat dla przystosowania go do swoich potrzeb. Bankomat najczęściej obdarzamy całkowitym zaufaniem, podczas gdy może on służyć przestępcom.

Istotnymi elementami, na jakie należy zwrócić uwagę przed przystąpieniem do wypłaty pieniędzy z bankomatu, są:

- wlot urządzenia do obsługi karty płatniczej – oryginalny czytnik kart,
- klawiatura do autoryzacji transakcji kodem PIN,
- górna część bankomatu – różnego rodzaju listwy i nakładki z logo kart płatniczych, gadżety z logo bankomatu – mogą ukrywać miniaturowa kamerę, która skierowana na klawiaturę bankomatu ma za zadanie "zarejestrować" wprowadzany przez osobę wypłacającą gotówkę kod PIN.

Przestępców interesują jedynie takie dane jak: numer karty płatniczej, data ważności oraz kod PIN. Są to dane niezbędne do przeprowadzenia transakcji zarówno w sieci Internet oraz w bankomacie. Urządzenia przedstawione na załączonych fotografiach pozwalają w zupełności na zdobycie przedmiotowych danych.

Urządzenia skanujące karty – pospolicie nazywane "skimmeram"i – mogą pozostać zainstalowane na bankomacie na czas do kilkudziesięciu godzin. Czas ich pracy uzależniony jest od zastosowanego zasilania oraz ilości dostępnej pamięci. Podczas wkładania karty do bankomatu, pasek magnetyczny zostaje sczytany i zapisany na widocznej karcie pamięci.
Budowa urządzenia nie jest skomplikowana, natomiast samo zainstalowanie tych elementów na bankomacie zajmuje kilka sekund.
Alternatywną metodą zdobycia PIN-u jest zastosowanie nakładki z minikamerą. Nakładkę taką umieszcza się nad klawiaturą numeryczną bankomatu w ten sposób, aby widoczna była ręka klienta "wstukująca" kod PIN, w celu autoryzacji transakcji. Najczęściej stosuje się w tym celu specjalnie dopasowane banery reklamowe lub listwy z logo poszczególnych systemów kart płatniczych. W ich wnętrzu umieszcza się mikrokamerę, której "oczko" ukrywane jest dla zamaskowania, np. w miejscu po mocowaniu śrubki.

Prosimy aby osoby korzystające z bankomatów przed wypłata pieniędzy zwróciły szczególną uwagę na to jak wygląda bankomat a w przypadku zauważenia jakiś przeróbek natychmiast powiadomiły policję.