kasia szymczak

Fałszywych kart płatniczych błyskawicznie przybywa

Skok na wirtualne pieniądze

Coraz powszechniej korzystamy z kart płatniczych. To nowoczesne, modne i rzekomo konieczne. Podobno to też bezpieczniejsze niż noszenie papierowych pieniędzy. Czy aby na pewno?

Piotr Dębek

Użytkowników plastikowych pieniędzy przybywa szybko, ale jeszcze szybciej przybywa oszustów rabujących elektroniczne pieniądze. W latach 1997–1999 zatrzymano w Polsce cztery grupy przestępcze zajmujące się fałszowaniem kart płatniczych. Według danych pochodzących ze Związku Banków Polskich aktualnie w Polsce w obiegu znajduje się 4500–5000 sztuk podrobionych, sfałszowanych i skradzionych kart płatniczych. Zdaniem policji tego typu przestępstw przybywa w tempie 300% rocznie – szybciej niż samych kart. Będzie więc jeszcze gorzej.

Historia pewnej szajki

Jedna z głośniejszych spraw ostatnich miesięcy rozpoczęła się i zakończyła we Wrocławiu. Jak się okazuje, elektroniczni złodzieje nie potrzebują ani zaawansowanej wiedzy, ani szczególnie wyrafinowanych urządzeń technicznych, a istniejące zabezpieczenia są niewystarczające.

W stolicy Dolnego Śląska działała grupa, która pod pozorem kontroli bankomatów firmy NCR montowała w nich miniaturowe kamery, urządzenia odczytujące kod pasków magnetycznych oraz przekaźniki transmitujące te dane drogą radiową. Uzyskiwane tą metodą (tzw. skimming) dane służyły do produkcji własnych kart płatniczych. Falsyfikaty powstawały na maszynie... domowej roboty. Mózgiem grupy był człowiek legitymujący się ukończeniem... technikum elektronicznego.

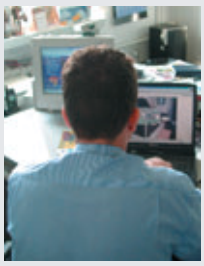
SPREPAROWANY BANKOMAT – listwa z reklamami została doczepiona przez przestępców i zawierała wbudowaną kamerę oraz przekaźnik radiowy.

To wystarczyło jednak, by grupa w ciągu trzech miesięcy, wykorzystując dane ze 160 kart, zagarnęła pół miliona złotych. Nie był to wcale wynik rekordowy – wręcz przeciwnie, przestępcy działali wyjątkowo ostrożnie, często zmieniając rejon działania i robiąc sobie wielodniowe przerwy w „pracy". Zawsze przez pewien czas zbierali dane o numerach kart, po czym realizowali je hurtowo w bankomatach jednej nocy. Za każdym razem podejmowali pieniądze w innym mieście.

Rozpracowaniem grupy zajmował się podkomisarz Piotr Zawadzki z Wydziału do Walki z Przestępczością Gospodarczą Komendy Wojewódzkiej we Wrocławiu. Finalny sukces możliwy był dzięki współpracy z bankiem, którego fachowcy dzień i noc monitorowali system informatyczny, czekając na sygnał, że w którejś z placówek dzieje się coś niezwykłego. Gdy wreszcie taki sygnał nadszedł, dalsze wydarzenia przypominały amerykański film sensacyjny. Policjanci ruszyli, mając świadomość, że na dojechanie na drugi koniec miasta, gdzie szajka opróżniała właśnie bankomat, pozostały im jedynie minuty. „Jadąc tam, złamałem chyba wszystkie przepisy ruchu drogowego" – wspomina Piotr Zawadzki. – „Dobrze, że był to środek nocy i ruchu na ulicach niemal nie było".

Wywiad

Czas fałszerzy



Rozmowa z podkomisarzem Piotrem Zawadzkim z wrocławskiej Komendy Wojewódzkiej Policji

CHIP: Czy pojawiają się jakieś nowe mody wśród oszustów?
Zawadzki: W ostatnim roku lawinowo przybywa przestępstw związanych z kartami płatniczymi. Wiąże się to ze zwiększeniem popularności „plastiku" oraz ubożeniem społeczeństwa. Do działań przestępczych wykorzystywane są osoby, które nie mają nic do stracenia – lumpy bez majątku, dla których odsiadka to wakacje. Są oni „preparowani" przez grupy przestępcze (np. elegancko ubierani) i wysyłani do banków, gdzie zakładają legalne konto i uzyskują kartę płatniczą. Przekazują ją następnie członkom szajki, którzy modyfikują kartę i, wykorzystując jej autentyczność, oszukują banki.

To urządzenie do zapisywania PASKÓW MAGNETYCZNYCH kart płatniczych pozwoliło wyłudzić pół miliona złotych.

Przestępcy zostali zatrzymani na gorącym uczynku. Grozi im od 5 do 15 lat więzienia.

W ostatnich dniach wrocławscy policjanci odnotowali kolejny sukces – jedynie dwa dni zajęło im wykrycie i likwidacja grupy Ukraińców, którzy – dysponując dobrze podrobionymi fałszywkami – robili zakupy w hipermarketach. W tym czasie zdążyli naciągnąć sklepy na kilkadziesiąt tysięcy złotych.

Tysiące okazji dla złodzieja

Trików pozwalających wyciągnąć pieniądze jest bez liku: od fałszywych stron banku, zachęcających do podania numeru karty i PIN-u, w celu sprawdzenia stanu konta, po stosowane w sklepach i restauracjach miniaturowe skanery kart kredytowych. Najmniejsze z owych urządzeń dają się ukryć w dłoni. Teraz wystarczy, byśmy przekazali nieuczciwemu kelnerowi nasz e-portfel, a on, niosąc go do czytnika, na naszych oczach zeskanuje kartę. Reszta jest już prosta – urządzenia do produkcji duplikatów plastikowych pieniędzy można kupić – jeśli wie się, gdzie – od 4000 dolarów. Nieco więcej kosztuje zestaw pozwalający przygotować również odpowiednie, kolorowe nadruki. Taka podróbka pozwala oszukać nie tylko bankomat, ale też sprzedawcę w sklepie. Technologia fałszowania i podrabiania kart nie jest skomplikowana, koszty niewielkie, a zyski olbrzymie.

Nieco inną praktykę zdarza się stosować pracownikom hipermarketów, zwłaszcza ochroniarzom. Ustawiają oni kamery bezpieczeństwa tak, by móc obserwować konsolę do autoryzowania transakcji bezgotówkowych przy kasie. Jeśli klient zapłaci kartą i wpisze PIN, pracownicy sklepu odszukują numer karty w systemie informatycznym sklepu i na podstawie czasu realizacji transakcji zestawiają go z odtworzoną z wideo sekwencją wpisywania kodu.

Czy są jakieś dobre wiadomości? Owszem. Zdaniem podkomisarza Zawadzkiego mało nadużyć popełnianych jest przy okazji handlu internetowego. Może wydawać się to paradoksem, ale tradycyjne zakupy płacone „plastikiem" wiążą się z większym ryzykiem niż transakcja online. Zawadzki określa wręcz patologie wokół sklepów sieciowych jako problem marginalny.

„U nas nic się nie stało"

Problemem w zwalczaniu przestępczości związanej z kartami płatniczymi są priorytety instytucji finansowych: większość z nich woli pogodzić się ze stratami, niż narazić reputację. Banki i towarzystwa ubezpieczeniowe nie są skore do ujawniania problemów z bezpieczeństwem swoich systemów informatycznych, a koszty strat mają wliczone w roczne budżety. Na szczęście zmniejsza się niechęć do współpracy z organami ścigania. Podinspektor Jan Hajdukiewicz, kierujący w Komendzie Głównej Policji zespołem do zwalczania przestępczości komputerowej i intelektualnej, potwierdza zmianę w nastawieniu instytucji finansowych: „Przez cały 2000 rok napłynęło do nas ponad 20 oficjalnych zgłoszeń od instytucji. W tym roku tyle samo mieliśmy w ciągu pierwszych dwóch miesięcy".

Problemy stróżom prawa stwarzają też nieprecyzyjne przepisy. Zdarza się, że instytucje odmawiają udzielenia informacji mogących pomóc w śledztwie, zasłaniając się... ustawą o ochronie danych osobowych. Oczywiście nie wstrzymuje to dochodzenia, ale tłumaczenie urzędnikom przepisów spowalnia pracę policji.

Policja kontratakuje

Przy KG Policji działa 11-osobowy zespół, kierowany przez podinspektora Jana Hajdukiewicza, który zajmuje się m.in. ściganiem przestępstw popełnianych przy użyciu kart płatniczych, ale także piractwem komputerowym, fonograficznym i audiowizualnym 24 »

Wywiad

Przestępstw elektronicznych będzie przybywało

JAN HAJDUKIEWICZ, kierownik zespołu w Komendzie Głównej Policji, zajmującego się zwalczaniem przestępczości komputerowej i intelektualnej

CHIP: Jak duża jest rzeczywista, nie zgłaszana liczba przestępstw związanych z włamaniami do instytucji?
Hajdukiewicz: Przypuszczam, że oficjalne liczby należałoby pomnożyć przez 10.
CHIP: Czy rozmiary tego zagrożenia są już na tyle duże, że mogą w znaczący sposób wpłynąć na gospodarkę kraju?
Hajdukiewicz: W tej chwili sytuacja nie jest jeszcze aż tak zła i przypuszczam, że uniknniemy tego. Myślę, że zdążymy się przygotować. Już się przygotowujemy. Należy jednak zdawać sobie sprawę, że tego typu przestępczość będzie wzrastała i osiągnie takie same rozmiary jak w Niemczech, Anglii czy USA. U nas są zdolni przestępcy, działają też np. Rosjanie. Trzeba również pamiętać, że ataki na nasze instytucje finansowe mogą wychodzić nie tylko z Polski, ale z dowolnego miejsca na świecie.
CHIP: Jaka jest wykrywalność tego typu przestępstw?
Hajdukiewicz: Wykrywalność jest uzależniona od dwóch rzeczy: dobrej woli i chęci współpracy poszkodowanego oraz szybkości zgłoszenia się do nas. Dobrze jest, jeśli ofiara przestępstwa wie, jakie materiały dowodowe trzeba zabezpieczyć, i niechcący sama nie zatrze śladów. Na przykład w przypadku włamania do komputera przede wszystkim trzeba zabezpieczyć wszystkie logi.
CHIP: Czy skuteczny, ostrożny i dysponujący dużą wiedzą cyberwłamywacz ma szansę pozostać bezkarny?
Hajdukiewicz: Nie ma możliwości niepozostawienia po sobie śladu, a w takich sytuacjach policja współpracuje z administratorami serwerów i dostawcami Internetu.
CHIP: Czy istniejące regulacje prawne wystarczają do zwalczania nowych typów przestępstw?
Hajdukiewicz: Myślę, że tak, ale technologie cyfrowe rozwijają się tak szybko, że w każdej chwili może się okazać, że rzeczywistość przerośnie wyobrażenia tych, którzy tworzyli prawo.
CHIP: Czy wprowadzenie w życie rozporządzenia nakładającego na dostawców usług internetowych obowiązku udostępniania wszystkich danych policji ułatwiłoby Panu życie?
Hajdukiewicz: Być może, ale bez niego da się robić to wszystko, co robimy do tej pory.
CHIP: Czego potrzebuje policjant, by zwalczać przestępstwa komputerowe?
Hajdukiewicz: Wiedzy, wiedzy i jeszcze raz wiedzy. Poza tym sprzętu i oprogramowania, a policja potrzebuje pieniędzy, żeby to wszystko mogła mu zapewnić.

Porady

Co robić, gdy Cię obrobią?

Jeśli padniemy ofiarą elektronicznych złodziei, powinniśmy natychmiast zgłosić ten fakt w najbliższej jednostce policji. Dodatkowo, z uwagi na to że funkcjonariusze w mniejszych miejscowościach mogą być nieprzygotowani do ścigania sprawców „cyfrowych" przestępstw, można poinformować o tym fakcie zespół ds. zwalczania przestępczości komputerowej i intelektualnej Komendy Głównej Policji w Warszawie. W przypadku oszustwa związanego z kartami płatniczymi należy zadzwonić pod numer (22) 601 47 40 lub (22) 601 31 12, natomiast ofiary włamania powinny zatelefonować pod numer (22) 601 27 47 lub (22) 601 27 49 (to numery telefonii stacjonarnej). Specjaliści z KGP będą mogli wówczas zaoferować pomoc lokalnym stróżom prawa.

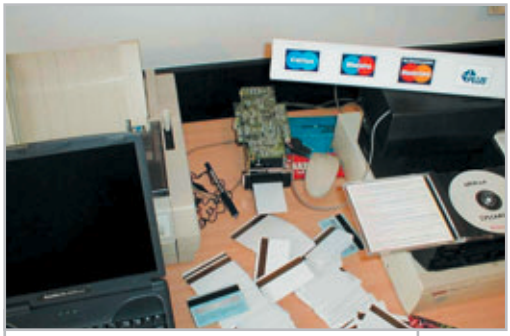
oraz hakerstwem. Zadaniem tym zajmują się zarówno informatycy z dyplomami wyższych uczelni, jak i pasjonaci, którzy nie ustępują wiedzą profesjonalistom. Ponadto w kilku komendach wojewódzkich są specjaliści zajmujący się tą dziedziną, blisko współpracujący z zespołem warszawskim. Policja korzysta też z usług cywilnych konsultantów.

W ciągu dwóch lat we wszystkich byłych miastach wojewódzkich ma zostać utworzone 50 stanowisk dla policjantów zajmujących się zwalczaniem przestępstw elektronicznych. Będą oni podlegali komendantom wojewódzkim, ale będą też ściśle współpracowali z zespołem warszawskim. W ten sposób powstanie ogólnokrajowa sieć na komputerowych złoczyńców. Zdaniem Jana Hajdukiewicza taka liczba fachowców w mundurach wystarczy do zapewnienia nam e-bezpieczeństwa: „Proporcjonalnie do liczby mieszkańców kraju tylu specjalistów mają też kraje sąsiednie: Niemcy, Francja i Anglia" – wyjaśnia szef warszawskiego zespołu antyhakerskiego – „Nie dopuścimy do tego, by cyfrowe podziemie zaczęło spychać w dół legalnie działające firmy".

Trzeba dodać, że taka liczba policyjnych fachowców wystarczy tylko pod warunkiem „uzbrojenia" ich w niezbędny, kosztowny sprzęt i oprogramowanie. Stworzenie takiego ogólnopolskiego teamu, wyposażenie go i wyszkolenie wymagają olbrzymich pieniędzy. Projekt ma już 3 lata i nie został do tej pory zrealizowany. Miejmy nadzieję, że pomimo kryzysu finansowego państwa środki na to wreszcie się znajdą.

Nakłady na nowoczesny sprzęt dla policji nie imponują. Nie brakuje w Polsce komend wojewódzkich policji, które w ogóle nie mają dostępu do Internetu. Nowoczesne notebooki pojawiają się wówczas, gdy ufundują je sponsorzy, np. instytucje finansowe i ubezpieczeniowe, które są zainteresowane zwiększeniem sprawności stróżów prawa w zakresie ścigania przestępstw komputerowych. Szkoda, że nie każdy uwolniony od szajki fałszerzy bank rewanżuje się swym zbawcom, fundując im sprzęt do pracy.

„Zinformatyzowanie" stróżów prawa ma także kolosalne znaczenie w walce z innego typu wykroczeniami. „W Australii 90% dowodów w sprawach karnych pochodzi z komputera" – wskazuje Andrzej Adamski, profesor prawa z uniwersytetu w Toruniu, specjalista prawa komputerowego.



Stanowisko pracy fałszerza w chwilę po wejściu policji: urządzenie zapisujące karty (u góry), sterujący nim notebook, sterta czystych „plastików" i fałszywa listwa reklamowa.

Pruszkow.com.pl

Skoordynowane działania na terenie całego kraju, zmierzające do zapewnienia porządku w cyberprzestrzeni, są konieczne. Istnieją przesłanki, iż elektroniczną przestępczością interesują się mafie. Można przypuszczać, że zorganizowane grupy przestępcze już korzystają z Sieci. „Prymitywni są ci, którzy z kijami bejsbolowymi wymuszają haracze, ale kierują nimi ludzie inteligentni" – tłumaczy podinspektor Hajdukiewicz. – „Oni wiedzą, że zarówno zwykły telefon, jak i komórkę można podsłuchać. Trudno przypuszczać, by nie wyciągnęli z tego wniosku i nie wykorzystywali Internetu do przesyłania zakodowanych np. PGP wiadomości. Nie ma na to bezpośrednich dowodów, ale gdy dawno temu mówiłem, że Wołomin i Pruszków kontrolują wytwórnie płyt i kaset z muzyką disco polo, też nie było na to dowodów".

Udowodnij, że nie jesteś złodziejem!

Odzyskiwanie pieniędzy utraconych w wyniku działań e-złodziei jest trudne. Trzeba zacząć od udowodnienia, że... nie ukradliśmy ich sami. Musimy przekonać bank, że nie mieliśmy nawet możliwości wybrania ich osobiście. Jest to możliwe, jeśli złodziej był tak miły, że korzystał z bankomatów na drugim końcu kraju. Gorzej, gdy oszust pobierał pieniądze w naszym rodzinnym mieście. W przypadku wątpliwości banki chętnie bronią się zastrzeżeniem, że nie ponoszą odpowiedzialności za transakcje wykonane przy użyciu PIN-u.

Urządzenie kopiujące pasek magnetyczny karty bez trudu mieści się w dłoni i nie jest skomplikowane.

Ta wymówka jest bardzo przydatna nie tylko wówczas, gdy ktoś skradnie nam kartę, podrobi ją, podejrzy wpisywany PIN lub uzyska go wskutek włamania do systemu informatycznego banku. Także reklamację niepoprawnego działania bankomatu da się odrzucić, wykorzystując powyższą formułę. Niekiedy jedynym sposobem odzyskania pieniędzy jest proces sądowy.

Tylko papier nie kłamie

Czy można jakoś zapobiec kłopotom? Najlepiej zachowywać wydruki z transakcji bankomatowych, notować każdorazowo zapłatę kartą i analizować comiesięczne wydruki bilansu konta. Warto też korzystać z oferowanej przez niektóre banki możliwości każdorazowego informowania e-mailem o zmianie stanu konta.

Jak łatwo zauważyć, jedynym sposobem kontrolowania, co dzieje się z naszymi elektronicznymi pieniędzmi, jest regularne sprawdzanie dokumentacji, także papierowej. Choć zakrawa to na paradoks, w dobie powszechnej digitalizacji zaufanie można mieć tylko do papieru. ■

Imię i nazwisko podkomisarza Piotra Zawadzkiego zostało zmienione.