Złodzieje wirtualnych pieniędzy

15 września 2009

Wirtualny rynek wraz ze wszystkimi usługami świadczonymi on-line ma dziś spory udział w sektorze gospodarki. Właśnie dlatego przestępstwa finansowe coraz częściej przenoszą się do wirtualnej rzeczywistości.

Internet jest dziś nie tylko źródłem wiedzy i rozrywki, jednym z kanałów komunikacji, ale także narzędziem, dzięki któremu jesteśmy w stanie zarządzać naszymi finansami. Wirtualny rynek wraz ze wszystkimi usługami świadczonymi on-line ma dziś spory udział w sektorze gospodarki. Właśnie dlatego przestępstwa finansowe coraz częściej przenoszą się do wirtualnej rzeczywistości.

Powodem do dumy w środowisku hakerów jest liczba kart kredytowych, których dane udało im się wykraść. Wirtualne pieniądze są niezwykle łakomym kąskiem dla tych, którzy chcą się wzbogacić w stosunkowo szybki sposób. Dodatkową zachętę stanowi również fakt, że wykrywalność tego typu przestępstw jest nadal bardzo niska, a ofiara praktycznie nie ma szans dochodzić swoich roszczeń. Szara strefa gospodarki, zorganizowana w sieć profesjonalnych oszustów i złodziei przeżywa więc w ostatnim czasie dynamiczny rozwój. Jak podaje najnowszy raport G Data Software, „podziemne" fora i giełdy dosłownie pękają w szwach od ofert handlarzy, oferujących dane do kart kredytowych, czy hasła dostępu do systemu PayPal oraz eBay. Stosunkowo nisko wyceniono zaś informacje służące do logowania na konta w grach on-line. W tym przypadku, nową tożsamość możemy kupić sobie już za 2 euro!

TOŻSAMOŚĆ NA SPRZEDAŻ

Schemat działań zawsze wygląda tak samo. Wykradając nasze prywatne dane, przestępca wystawia następnie loginy oraz hasła

dostępu do kont w formie oferty na czarnym rynku. Proceder jest już na tyle rozwinięty, że na Zachodzie powstały sklepy on-line oferujące skradzioną tożsamość, a poszczególni handlarze udzielają rabatów ilościowych dla tych, którzy zainteresowani są zakupem większej liczby haseł dostępu.

Jeżeli „klient" jest niezadowolony, skradzioną tożsamość zawsze można wymienić, a płatności za zakup dokonuje się za pomocą popularnych na czarnym rynku usług płatniczych, takich jak Western Union, Paysafecardf czy Webmoney.

ZAKUPY NA TWÓJ RACHUNEK

Sposobów na przejęcie wirtualnej tożsamości jest wiele. By zdobyć dostęp do naszych danych, wirtualni złodziej korzystają z takich narzędzi jak phishing (tworzenie fałszywych stron bankowych, do których link rozsyłany jest za pomocą poczty), konie trojańskie, czy po prostu włamując się do on-line-owych baz danych. Inną metodą jest skimming, czyli skanowanie kart bankomatowych. Tego typu kradzieże wymagają jednak od złodzieja podjęcia działań poza siecią. Skradzione w ten sposób dane można z powodzeniem wykorzystywać w celu dokonywania zakupów online. Ogromną popularnością w środowisku przestępców cieszą się tak zwane „cardable shops", czyli sklepy, w których ilość danych wymaganych do złożenia zamówienia i zapłacenia za towar jest minimalna. „Nic więc dziwnego, że na czarnym rynku największą wartość mają te konta, do których przestępca zgromadził najwięcej danych" – tłumaczy Tomasz Zamarlik z G Data Software.

INFORMACJE WARTE MILIONY

Dane do kart kredytowych to jednak tylko wierzchołek góry lodowej. Posiadając tego typu informacje, cyberprzestępcy mogą uzyskać za pomocą tak zwanych generatorów kart kredytowych, kolejne numery kart płatniczych należących do danego banku. Wirtualni złodzieje mogą w ten sposób wyczyścić twoje konto, nawet wtedy, gdy nie jesteś bezpośrednią ofiarą przestępstwa.

Na zagranicznych forach internetowych znaleźć można cenniki podające sumę pieniędzy za jaką można kupić interesujące nas konto. Najdroższe są wszelkiego rodzaju bazy danych pochodzące między innymi z e-sklepów oraz listy adresów e-mail do zdefiniowanej grupy użytkowników (np. klientów banku). Za taki wykaz niejednokrotnie trzeba zapłacić blisko 250 euro. Dziesięciokrotnie mniej należy wydać, by uzyskać dane do konta w systemie PayPal czy click & buy.

BEZPIECZNY BANKOMAT – NA CO ZWRACAĆ UWAGĘ?

Wspomniany już wcześniej skimming to coraz popularniejszy proceder nawet na polskim rynku. Instalując w bankomacie dodatkowy czytnik kart oraz kamerę przestępca gromadzi informacje na temat numeru karty płatniczej oraz hasła PIN niczego nieświadomej ofiary. Niezbędny sprzęt można z łatwością kupić na aukcjach internetowych za kilka tysięcy złotych. Znając dokładne wymiary bankomatu, złodzieje są w stanie dołączyć do niego urządzenia, które wizualnie doskonale wkomponują się w całość, tak, że standardowy klient banku nie jest w stanie rozpoznać zagrożenia. Na szczęście ze względu na jawność działania oraz dodatkowy monitoring bankomatów, wykrywalność tego typu przestępstw jest stosunkowo wysoka. Coraz częściej zdarzają się również telefony od zaniepokojonych klientów, którzy alarmują o nowych urządzeniach dołączonych do bankomatu.

Tym co powinno niepokoić, są dodatkowe mechanizmy umieszczone w miejscu, gdzie wprowadza się kartę. Wprowadzając kod PIN zawsze warto zakryć klawiaturę drugą ręką lub po prostu wykonać kilka dodatkowych (fałszywych) ruchów. Wszelkie wątpliwości należy bezwzględnie zgłaszać do najbliższych placówek bankowych lub po prostu dzwoniąc na policję.

UWAŻAJ NA PŁATNOŚCI ON-LINE

Stworzenie fałszywej strony bankowej to jedna z popularniejszych metod na zyskanie danych umożliwiających

dostęp do internetowych kont. Wykorzystując własną sieć bonet, przestępca rozsyła następnie wiadomości e-mail zawierające link do witryny z prośbą o zalogowanie się do systemu np. w celu weryfikacji danych przez system bankowy. Wpisując autentyczne dane na stronę stworzoną przez złodzieja, umożliwiamy przestępcy zgromadzenie pokaźnej bazy danych, które następnie wykorzystuje on w celu dokonania między innymi zakupów obciążając nimi nasz rachunek. Jak czytamy we wspomnianym raporcie G Data, technika ta, zwana w skrócie phising, staje się popularnym narzędziem również w przypadku serwisów bukmacherskich, kasyn czy kont założonych na My Space.

By nie pozwolić się okraść z własnej tożsamości, należy zawsze bardzo ostrożnie posługiwać się swoimi danymi. Przed wpisaniem informacji trzeba sprawdzić czy strona jest chroniona (symbol kłódki), a w przypadku wątpliwości dobrze jest skonsultować się z infolinią obsługującego nas banku. Należy również pamiętać, że instytucje finansowe prawie nigdy nie wymagają wirtualnej weryfikacji danych od swoich klientów. Zanim klikniemy na link – dokładnie porównajmy go z adresem, z którego do tej pory korzystaliśmy. Nawet jeżeli nie zalogujemy się na fałszywej stronie, nie wykluczone, że na naszym komputerze zainstaluje się jakiś złośliwy program pobierający.

Technologie internetowe niewątpliwie będą się rozwijać. Wraz z tym zapewne nadal będą pojawiały się nowe zagrożenia. Dlatego korzystając z Sieci pamiętajmy, że wirtualna rzeczywistość, chociaż tak bardzo pasjonująca, bywa również niezwykle niebezpieczna.

Autor: Urszula Niemiec
Źródło: iThink