POLICJA PODLASKA

https://podlaska.policja.gov.pl/pod/dzialania/przestepczosc-gospodar/struktura-wydzialu/zespol-ii/bankowosc-elektroniczna/28418,Bankowosc-elektroniczna-zagrozenia.html
2020-09-28, 11:15

BANKOWOŚĆ ELEKTRONICZNA - ZAGROŻENIA

Oskubani w sieci

Uważasz, że na twoim pececie nie ma wirusów? I pewnie też, że nigdy nie dałeś się nabrać na phishing? Śnij dalej! Już od dawna hakerzy używają zupełnie nowych metod, które stanowią nie lada wyzwanie nawet dla tych najbardziej doświadczonych użytkowników.

Trzymanie gotówki w banku daje nam coś tylko wtedy, gdy nikt nam jej nie ukradnie. To oczywiste. W artykule, na podstawie aktualnych wydarzeń pokazujemy jednak, że jeśli chodzi o pieniądze, nie możemy ufać ani naszemu bankowi, ani przyjaciołom, ani nawet własnemu pecetowi. Co gorsza, problemem jest w tym przypadku nie tylko niefrasobliwość internautów, którzy nabierają się na phishing, ale także możliwość zhakowania globalnego systemu rozliczeń finansowych, którego zasięg – jak miało to miejsce w styczniu u naszych zachodnich sąsiadów – może objąć cały kraj.

Phishing w serwisach społecznościowych

Jak ważne jest niezawodne oprogramowanie bankowe, pokazują dramatyczne przykłady z życia. Trafiając na coraz lepiej poinformowanych internautów, hakerzy sięgają po zupełnie nowe metody, a one potrafią wyprowadzić w pole nawet doświadczonych użytkowników. Na przykład za pomocą nowego triku na Facebooku. Okazuje się bowiem, że współczesne trojany przechwytują nie tylko loginy i hasła do e-banków oraz kody PIN, ale także informacje dostępowe z Facebooka.

Technowinki na FacebookTe ostatnie są często chronione w stopniu o wiele niższym niż informacje bankowe, co pozwala oszustom na więcej niż tylko wgląd w prywatne dane użytkownika, mogą np. łatwo ustalić bezpośrednich znajomych przejętego konta i przesłać im odsyłacze do sfałszowanych czy zainfekowanych stron. Większość adresatów nigdy nie kliknęłaby linku phishingowego w spamowej poczcie – są na to już zbyt wyedukowani – ale z reguły nie mają obiekcji, aby sprawdzić treść odnośnika, który podsyła im użytkownik będący jego znajomym na Facebooku.

Ale to nie wszystko, mając nielegalny dostęp do konta na Facebooku, przestępca może na przykład publikować sfałszowane strony na Allegro i polecać zainfekowane trojanami witryny z darmowym oprogramowaniem albo filmiki na YouTube zawierające złośliwe kody. Przez usługi skracania adresów, np. TinyURL, które na Twitterze i Facebooku są czymś zwykłym, kanciarz może kierować użytkowników tych serwisów do fałszywych domen.

Również sztuczki, na które w wydaniu emailowym nikt się już nie nabiera, w wydaniu serwisów społecznościowych wyglądają całkiem obiecująco. Prosty przykład: po zhakowaniu konta ofiary oszust wysyła do jej przyjaciół bezpośrednią prośbę o wsparcie. Mami ich informacjami, że ich przyjaciel na urlopie jest w kłopotach finansowych (skradziony paszport, wypadek i wysokie koszty leczenia itp.) i pilnie potrzebuje gotówki. Najlepiej w ciągu kilku minut – sytuacja jest krytyczna – przelewem przez pośrednika w transferach pieniężnych takich jak Western Union. Skutek: pieniądze trafiają w ręce złodzieja.

Przechytrzony przez system

E-banki nie zawsze są skłonne do płacenia za straty, jakie ponoszą ich klienci, stając się ofiarami hakerskich ataków. Pokazuje to przypadek Tomasza Zabielskiego (imię i nazwisko zmienione przez redakcję) – jednego z czytelników CHIP-a będącego obecnie na emigracji w Niemczech, który zreferował nam to, co go spotkało.

Tuż po przyjeździe do Berlina, gdzie znalazł pracę jako administrator sieci korporacyjnej w dużej filmie handlowej, musiał założyć konto bankowe. Zdecydował się na jedną z bardziej szacownych instytucji – duży niemiecki bank spółdzielczy. Instytucja ta używała do podpisywania zleceń metody eTAN. Jest do niej konieczne urządzenie przypominające token, które generuje po naciśnięciu przycisku numer TAN (Transaction Authentication Number) uwierzytelniający transakcję.

Ten sposób przez wiele lat uważany był za bezpieczny, ponieważ TAN jest mocno związany z danymi adresata przelewu. Jeśli oszust próbuje przekierować przekaz pieniędzy na inne konto, numer TAN staje się nieważny dla tej transakcji. Luki tej metody udowodniła jednak firma RedTeam Pentesting zajmująca się zabezpieczeniami komputerowymi, której w 2009 r. za pomocą specjalnego trojana udało się obejść mechanizm eTAN.

Ale Zabielski już kilka miesięcy wcześniej odczuł na własnej skórze, że metoda eTAN nie jest tak pewna, jak to się powszechnie uważa – dokonał dwóch przelewów, które po realizacji wyświetlały się prawidłowo w online'owym systemie transakcyjnym banku. Zabielski nie był nowicjuszem w branży komputerowej – zawód admina wykonywał już od ponad 10 lat. Nie padł też ofiarą phishingu, a jego pecet był wystarczająco zabezpieczony. Gdy jednak zalogował się do banku kilka dni później, dostrzegł, że druga transakcja trafiła nie tam, gdzie trzeba – podmieniony odbiorca okazał się hurtownią sprzętu komputerowego, o której Zabielski nigdy nie słyszał. Wcześniej firma ta otrzymała zwykłe zamówienie od domniemanych oszustów i po wpłynięciu pieniędzy wysłała im towary o wartości 1000 euro.

Lecz przedsiębiorstwo odmówiło podania Zabielskiemu danych klientów podejrzanych o malwersacje. Powód? Ochrona danych osobowych wzmocniona dodatkowo faktem, że nie miał obywatelstwa niemieckiego. Poszkodowany zadzwonił więc na infolinię banku, gdzie został poinformowany, że z numerami TAN należy się obchodzić ostrożnie. Poza tym truizmem ofiara dowiedziała się, że odzyskanie pieniędzy jest już niemożliwe, gdyż od zajścia minęła ponad doba, a bankowe dochodzenie kosztuje 16 euro płatne z góry. Ostatecznie bank zaproponował, by zwrócił się o pomoc do policji. Zabielski złożył doniesienie o popełnieniu przestępstwa. Od swego banku nie usłyszał już nic więcej – do czasu aż napisał do zarządu.

Odpowiedź instytucji finansowej, której powierzył przecież swoje środki, była lakoniczna: „Metoda eTAN jest bezpieczne, zatem to on musiał popełnić błąd. Jednakże ze względu na dobre stosunki handlowe bank zwróci mu utraconą kwotę". Dzięki temu, że nie dał się spławić, Zabielski dostał z powrotem swoje pieniądze. Nie udowodnił jednak, że zabezpieczenia banku są niewystarczające.

W jaki sposób kanciarze zdołali ostatecznie obrabować ofiarę, nie jest już do końca zrozumiałe – mimo intensywnego poszukiwania śladów na swoim pececie, Zabielski nie odnalazł na nim malware'u.

A musimy założyć, że chodziło o trojana, który został zamaskowany przez rootkita i ukrył się w systemie w sposób niemożliwy do wytropienia. Gdy ofiara weszła przez przeglądarkę na strony banku, trojan przekierował ją na fałszywkę. Zabielski nie zauważył ani drobnych różnic w wyglądzie stron, ani tych wynikających z podrobionego certyfikatu, nie był więc świadomy, że to, co bierze za witrynę banku, jest w rzeczywistości jej podróbką. Od tej pory wymiana danych odbywała się pomiędzy podrobioną witryną a nieświadomym niczego Zabielskim. Po wygenerowaniu i wprowadzeniu numeru TAN przestępcy przejęli go i uwierzytelnili nim własną transakcję – w tym przypadku był to przelew na konto firmy komputerowej. Z punktu widzenia Zabielskiego wszystko wyglądało jednak tak, jakby faktycznie składał dyspozycję przez system trakcyjny swojego banku.

Oskubany przez automaty

Jednak niebezpieczeństwo utraty pieniędzy ma miejsce nie tylko wtedy, gdy sami surfujemy po Sieci. Nawet podejmowanie gotówki w bankomacie wydaje się ryzykowne. Otóż na początku tego roku zmanipulowane albo zainfekowane trojanem bankomaty przechwytywały dane z kart. Winne temu były ich błędnie zaprogramowane chipy, co spowodowało, że 1 stycznia 2010 r. w Europie nieprawidłowo działało 30 mln kart kredytowych i debetowych.

Według oficjalnych informacji programy zaimplementowane w chipach były wykonywane w kolejności, która w połączeniu ze zmianą daty po 1 stycznia 2010 r. doprowadziła do zawieszenia systemu. Był to scenariusz, którego pomimo wyczerpujących testów wytwórca chipów – holenderska firma Gemalto – nie przewidział. Dla największych światowych oferentów kart chipowych był to duży problem. Tym bardziej że angielski ekspert ds. bezpieczeństwa

komputerowego Ross Anderson stwierdził, iż standard EMV rozwijany przez konsorcjum firm Europay International, MasterCard i VISA i stosowany w kartach chipowych jest zbyt skomplikowany i niepewny. Ponadto ekspert skrytykował prace inżynierskie przy tym projekcie i mierny poziom zarządzania jakością.

Andersonowi wspólnie z zespołem badawczym uniwersytetu w Cambridge udało się obejść uwierzytelnianie kodem PIN stosowane przy kartach kredytowych. Grupa ekspertów pokazała też, jak za pomocą prostych środków przechytrzyć terminal płatniczy, stosując atak Man-in-the-Middle. Jeden z bankomatów oszukano podrobioną kartą, przestawiając go na uwierzytelnienie za pomocą skanowania podpisu. W innym przypadku zmuszono terminal, aby wierzył, że wprowadzono prawidłowy PIN.

W jeszcze innym teście, który przeprowadzono w stołówce studenckiej uniwersytetu Cambridge, eksperci zmanipulowali lokalny system płatności, co doprowadziło do tego, że akceptował on dowolny PIN.

Dla Andersona jest jasne, że standard EMV jest mało bezpieczny. Największy problem stanowi jego złożoność. – Skomplikowanie algorytmu osiągnęło taki stopień, że nawet w branży nikt go dokładnie nie rozumie – twierdzi Anderson. – Banki, producenci terminali i kart płatniczych oraz programiści znają go tylko częściowo. Nikt nie panuje nad całością. Potwierdza to Salim Gueler z firmy Kobil System zajmującej się wytwarzaniem czytników kart do płatności online: – Jako wsparcie narzędziowe otrzymujemy jedynie SDK (Software Development Kit), który daje nam do dyspozycji interfejs, jakiego potrzebujemy. I na tym kończy się nasza wiedza o standardzie EMV.

Dla wielu programistów brak przejrzystości standardu nie jest jednak oznaką jego słabości. Wręcz przeciwnie, uważają, że bardzo trudno jest odkryć piętę achillesową tak złożonego systemu. Anderson jest jednak innego zdania: – Zwykła implementacja mechanizmu EMV nie zapewnia automatycznie poziomu bezpieczeństwa przewidzianego przez tę specyfikację. Trzeba założyć, że pojawią się kolejne luki, które pewnego dnia zostaną odkryte i wykorzystane przez hakerów.

Co ciekawe, doszło do sporu między różnymi wystawcami kart odnośnie zabezpieczeń: niemiecka centrala kredytowa oświadczyła, że dopuszczone przez nią do obrotu karty są bezpieczniejsze niż brytyjskie. Powód? Mechanizm EMV jest implementowany w Wielkiej Brytanii bezpośrednio na kartach. Tymczasem na niemieckich plastikowych pieniądzach działa system operacyjny SECCOS, a EMV jest w nim jedynie fragmentem oprogramowania. Dzięki temu złamanie go to bardziej skomplikowane zadanie niż przy kartach, których zabezpieczenia udało się obejść Andersonowi. Utrudnienia biorą się m.in. stąd, że niemieckie karty stosują dynamiczną autoryzację, a brytyjskie – statyczną.

Jednak Ross Anderson już teraz przewiduje, że niemieckie banki będą miały problem, gdy hakerzy rozwiną nowe technologie. Co więcej, jego zespół wziął pod lupę niemieckie karty kredytowe i wypunktował ich potencjalne słabości. Czy i w jakim stopniu angielski naukowiec miał rację, okaże się w najbliższej przyszłości.

Szok przy bankowej kasie

Awaria systemu płatności online to niejedyna sytuacja, w której zagrożone są nasze pieniądze. Może się bowiem zdarzyć, że bank odmówi wypłaty pieniędzy nawet z klasycznej książeczki oszczędnościowej. Powód? Tak kuriozalny, że trudno w niego uwierzyć: przedawnienie dodatniego salda.

CHIP-owi znany jest fakt, gdy jeden z zachodnich banków odmówił wypłaty pieniędzy naszemu czytelnikowi, ponieważ jego oszczędności leżały „odłogiem” zbyt długo – od 2001 r. Urzędnik zapewniał, że konta nie można znaleźć w systemie, a jego numer został przypisany do innej osoby. Co więcej, odmówił oddania petentowi książeczki oszczędnościowej, twierdząc, że ona też jest już nieważna. Dopiero po zdecydowanych żądaniach klient otrzymał jej poświadczoną kopię. Na możliwość podjęcia z niej pieniędzy musiał czekać znacznie dłużej – 8 tygodni, a bez niej przypuszczalnie nigdy nie odzyskałby już własnych środków.

Rzadko występujący przypadek, ale wcale nie jednostkowy. Innemu naszemu czytelnikowi także zabrano nieużywaną od lat książeczkę oszczędnościową, ale nie otrzymał na to pokwitowania. Kilka tygodni później, gdy chciał podjąć przypisane do niej środki, obsługujący go wtedy urzędnik stwierdził, że nigdy nie miał w ręku jego książeczki – pieniądze przepadły.

To nie jest odosobniony przypadek. Pracownik jednego z banków wyjawił, że raz do dwóch razy w roku musiał kierować zrozpaczonych klientów do działu reklamacji, ponieważ nieużywane konta były przepisywane na inne osoby. Według wypowiedzi urzędnika osoby odzyskiwały jednak swoje pieniądze, ponieważ w ramach reformy prawa zobowiązaniowego dodatnie saldo nie może się przedawnić. Banki, które stosowały inne praktyki, działały bezprawnie.

Ale wiele z nich znalazło inną drogę, aby pozbywać się nieużywanych kont. Gdy klient zakładał u nich rachunek oszczędnościowy, podpisywał zobowiązanie, że prowizje za jego obsługę będą znacząco wyższe, jeśli po określonym czasie na koncie nie będą księgowane żadne transakcje. W ten sposób banki do dziś pod osłoną prawa stopniowo uszczuplają środki na nieużywanych rachunkach.

Metoda Man-in-the-Middle przełamuje wszystkie zabezpieczenia

Atak Man-in-the-Middle (MITM) to ogromne zagrożenie dla naszych pieniędzy. Stosujący tę metodę, haker może bowiem przejąć kontrolę nad połączeniem z dowolnym e-bankiem, niezależnie od zabezpieczeń, takich jak tokeny, listy haseł jednorazowych czy zatwierdzania transakcji kodami przesyłanymi SMS-em.

W ataku MITM haker musi ustawić się jako ogniwo pośrednie pomiędzy pecetem ofiary a witryną jego banku, Aby to wykonać, przestępcy stosują sztuczki, takie jak podmiana pliku localhost, atak na lokalny serwer DNS czy tradycyjny phishing. Efekt tych zabiegów jest taki, że ofiara jest pewna, iż wchodzi na strony swego banku, a w rzeczywistości loguje się na fałszywkę.

strong>Typowy przebieg ataku

Po wejściu na podrobioną witrynę klient wpisuje swój login i hasło. Haker przejmuje je i w imieniu ofiary loguje się do banku. Bank w odpowiedzi odsyła kod HTML obrazujący aktualny stan konta. Haker retransmituje go do przeglądarki ofiary, ponieważ sama znajomość hasła i loginu najczęściej nie pozwala na transfer pieniędzy.

Taka wymiana danych trwa do momentu, gdy ofiara decyduje się na wykonanie operacji, którą musi uwierzytelnić przez stosowany w danym banku system zabezpieczeń taki jak odczyt z tokena, kod z listy haseł jednorazowych czy zatwierdzający transakcję SMS. Po przechwyceniu takiego zlecenia haker modyfikuje je, np. wysyłając do banku zlecenia przesłania wszystkich pieniędzy na inne konto. Bank w odpowiedzi przesyła SMS albo żąda hasła z listy. To żądanie jest przesyłane do ofiary, która jest przekonana, że zatwierdza własną transakcję, np. opłatę rachunku za prąd, gdy w rzeczywistości autoryzuje transakcję, która może wyczyścić jej konto do zera.

Ochrona przed Man-In-The-Middle

Aby przekierować nas na fałszywkę, hakerzy muszą zainfekować nasz system. Pierwszą linią obrony jest więc aktualizowany skaner antywirusowy. Dodatkowo powinniśmy zwracać na to, żeby strona banku miała aktualny certyfikat wydany przez znaną firmę taką jak VeriSign czy Thawte Inc. — wtedy bowiem wiemy, że logujemy się do oryginalnej witryny, a nie do podrobionej.

Źródło: CHIP.PL