Kompendium wiedzy na temat Trojanów bankomatowych - jak się ustrzec przed kradzieżą pieniędzy?

Z każdym dniem rośnie liczba doniesień o nowych atakach na bankomaty z wykorzystaniem złośliwego oprogramowania. Firma Doctor Web przygotowała zestawienie podstawowych informacji na temat tego rodzaju Trojanów.

W celu wykradzenia środków z rachunku bankowego, cyberprzestępcom wystarczy dziś znajomość numeru konta i kodu PIN karty płatniczej. Jednym ze sposobów na uzyskanie tego rodzaju danych jest zainfekowanie bankomatów złośliwym oprogramowaniem.

Obecnie w bazie wirusów Dr.Web zarejestrowano jak dotąd 25 wersji Trojanów bankowych z rodziny Trojan.Skimer, które pozwalają cyberprzestępcom na wykradanie danych kart oraz kodów PIN. Trojan.Skimer znany jest od 2009 r., a jego najnowsza wersja pochodzi z lutego 2014 roku.

Poszkodowany zazwyczaj dowiaduje się o kradzieży już po fakcie, ale istnieją sposoby, aby zapobiegać tego rodzaju incydentom. Bankom zaleca się korzystanie ze specjalnego oprogramowania antywirusowego, użytkownicy zaś powinni wiedzieć, jak minimalizować ryzyko utraty środków finansowych.

Specjaliści z firmy antywirusowej Doctor Web przygotowali kilka pomocnych informacji dla właścicieli kart płatniczych, wypłacających pieniądze z bankomatów:

1. Jak hakerzy mogą ukraść kod PIN do karty płatniczej?

Brak zainstalowanego programu antywirusowego, wykorzystywanie luk w systemie ochrony bankomatów oraz niska świadomość zagrożenia ze strony ich użytkowników pozwala cyberprzestępcom na wiele sposobów wyłudzać środki od klientów banków. Jednym z nich są specjalne urządzenia skimmer (czyli nakładka na klawiaturę) lub ukryta kamera, zamontowane przez przestępców. Urządzenia te mogą być montowane na zewnątrz lub wewnątrz bankomatów. Skimmer rejestruje dane zawarte na pasku magnetycznym karty, a za pomocą kamery złodziej odczytuje wprowadzany PIN. Kody PIN mogą zostać ukradzione w wyniku zainfekowania sieci korporacyjnej banku Trojanem z rodziny Trojan.Spy, a także poprzez zainfekowanie oprogramowania bankomatu.

2. Jak właściciel karty płatniczej może chronić się przed malware typu Trojan.Skimer?

Należy upewnić się, że bankomat nie jest wyposażony w ukryte kamery lub nie ma zainstalowanej specjalnej nakładki na klawiaturę. Podczas wpisywania kodu PIN, warto zakrywać drugą ręką klawiaturę.

Drugi rodzaj zagrożenia, czyli zainfekowanie bankomatu złośliwym oprogramowaniem, jest już praktycznie niemożliwe do wykrycia i uniknięcia przez przeciętnego użytkownika . Jedynie bank właściciel bankomatu może i powinien chronić bankomaty, wyposażając je w wyspecjalizowane oprogramowanie antywirusowe. Zanim dokonamy transakcji, należy upewnić się, czy czytnik kart nie wzbudza podejrzeń i czy do bankomatu nie są przymocowane żadne podejrzane urządzenia. Jeśli cokolwiek wzbudza nasze wątpliwości, nie powinniśmy korzystać z tego bankomatu.

3. Otrzymałeś
wiadomość tekstową: "Twoja karta bankowa jest zablokowana. Więcej informacji
pod numerem telefonu &.". Jak postąpić w takiej sytuacji?

Po otrzymaniu tego rodzaju wiadomości, należy od
razu zadzwonić na numer obsługi klienta w celu
uzyskania dalszych informacji. Warto pamiętać, żeby dzwonić tylko na oficjalne
numery banku (np. ten widniejący na stronie lub podany na odwrocie karty), a
nie ten z smsa, i nigdy nie podawać przez telefon kodu PIN. Tego rodzaju smsy
mogą być wysyłane przez cyberprzestępców w celu wyłudzenia od nas poufnych
danych (tzw. atak phisingowy).

4. W jaki sposób przestępcy mogą zainfekować bankomat
złośliwym oprogramowaniem?

Większość nowoczesnych bankomatów działa w
systemie Microsoft Windows, głównie Windows XP, którego wsparcie Microsoft zakończył
w kwietniu 2014 roku. W związku z tym bankomaty mogą być infekowane przez te
same rodzaje złośliwego oprogramowania, które wykorzystywane są do ataków na
komputery. W celu kradzieży pieniędzy z bankomatu lub z karty kredytowej, tworzone
są specjalne rodzaje złośliwego oprogramowania w postaci Trojanów bankowych.

Zainfekowanie bankomatu
może polegać na podłączeniu do tego urządzenia przez przestępcę zawirusowanej
pamięci masowej (przeważnie jest to pendrive USB), lub doprowadzeniu do
wykorzystania przez konserwatorów bankomatów zainfekowanych nośników danych.
Zdarzały się też przypadki załadowania i uruchomienia kodu wirusa z
odpowiednio spreparowanej karty serwisowej, i dzięki wykorzystaniu luk w
specjalistycznym oprogramowaniu tych urządzeń.5. Jak hakerzy
mogą uzyskać dane o kartach bankowych, wykorzystując w tym celu Trojany bankowe? W
trakcie korzystania z zarażonego bankomatu zostają zapisane informacje dostępne
na pasku magnetycznym oraz kod PIN. Odczytanie informacji przez złodzieja
odbywa się poprzez wprowadzenie odpowiednio spreparowanej karty, która pozwala
przejąć kontrolę nad urządzeniem, wyświetlając skradzione informacje na ekranie
lub zapisując je na użytej karcie. Dane mogą zostać również wydrukowane na
paragonie.

Głównym zagrożeniem, jakie niosą ze sobą tego
rodzaju Trojany bankowe jest to, że za pomocą skradzionych danych cyberprzestępcy zyskują
możliwość tworzenia duplikatów kart bankomatowych oraz kredytowych i wypłacania pieniędzy z kont
osób, które skorzystały z
zainfekowanych bankomatów. mówi specjalista Dr.Web,
Joanna Schulz-Torój. O ile zabezpieczenie bankomatów leży po stronie banku, w
przypadku skimmingu sami powinniśmy wykazać się ostrożnością, a w szczególności
pamiętać o podstawowych zasadach bezpieczeństwa. Warto również na bieżąco
sprawdzać saldo rachunków oraz wyciągi z kart i kont bankowych. dodaje
Joanna Schulz-Torój.