Czy czekają nas święta pod znakiem kradzieży pieniędzy online?

Kategoria: Aktualności
Opublikowano: wtorek, 03, grudzień 2013 23:00
Rafał Rudka
Odsłony: 1552

Eksperci z Kaspersky Lab odnotowali kilka tysięcy prób zainfekowania komputerów wykorzystywanych do bankowości online szkodliwym programem, którego twórcy twierdzą, że może on zaatakować "każdy bank w każdym kraju". Trojan bankowy Neverquest obsługuje niemal wszystkie znane sztuczki wykorzystywane przez cyberprzestępców do obchodzenia zabezpieczeń systemów bankowych: modyfikowanie kodu stron WWW, zdalny dostęp do systemu, socjotechnikę i wiele więcej. W świetle tego, że trojan ten posiada również możliwość samopowielania się, eksperci szacują gwałtowny wzrost ataków związanych z Neverquestem oraz istotne straty finansowe na całym świecie.

Tygodnie poprzedzające Boże Narodzenie i Nowy Rok to tradycyjnie okres wzmożonej aktywności cyberprzestępczej. Już w listopadzie na podziemnych forach pojawiły się ogłoszenia kupna i sprzedaży baz danych pozwalających na uzyskanie dostępu do kont bankowych i innych dokumentów umożliwiających zarządzanie kontami, na które można przelewać skradzione pieniądze. Neverquest pojawił się jeszcze wcześniej - ogłoszenie, w którym poszukiwano partnera do współpracy przy tym trojanie, zostało opublikowane na podziemnych forach już w lipcu bieżącego roku.

Siergiej Golowanow, główny badacz ds. bezpieczeństwa w Kaspersky Lab, komentuje: "Po zakończeniu kilku spraw związanych z tworzeniem i dystrybucją szkodliwych programów wykorzystywanych do kradzieży informacji o stronach bankowych na czarnym rynku pojawiło się kilka 'luk'. Nowi szkodliwi użytkownicy próbują wypełnić je nowymi technologiami i pomysłami. Neverquest to tylko jedno z zagrożeń, które powstało, by zająć miejsce okupowane wcześniej przez ZeuSa i Carberpa".

Neverquest kradnie nazwy użytkowników oraz hasła do kont bankowych oraz wszelkie dane wprowadzane przez użytkowników na stronach bankowych. Specjalne skrypty dla Internet Explorera oraz Firefoksa dbają o to, by skradzione informacje mogły płynnie trafiać do serwerów kontrolowanych przez cyberprzestępców. Lista atakowanych serwisów obejmuje 28 stron banków oraz systemów płatności z całego świata. Kolejna funkcja trojana pomaga atakującym w rozszerzaniu tej listy i tworzeniu kodu wstrzykiwanego do nowych stron, które wcześniej nie znajdowały się na celowniku.

Ze wszystkich stron atakowanych przez ten szkodliwy program najważniejszym celem dla cyberprzestępców wydają się być fundusze inwestycyjne. Serwisy te wyposażone są w wiele metod pozwalających klientom na zarządzanie swoimi finansami online. Daje to cyberprzestępcom nie tylko możliwość przelewania funduszy na własne konta, ale także pozwala im grać na giełdzie przy użyciu skradzionych kont i pieniędzy ofiar Neverquesta.

Ochrona przed zagrożeniami takimi jak Neverquest wymaga czegoś więcej niż oferują standardowe programy antywirusowe. Użytkownicy potrzebują rozwiązania zaprojektowanego z myślą o zapewnianiu ochrony transakcji finansowych online, które potrafi kontrolować procesy uruchomionych przeglądarek internetowych i uniemożliwia dokonywanie zmian w zainstalowanych aplikacjach przez inne programy.

Źródło: Kaspersky Lab