Kategoria: Styl życia
Opublikowano: poniedziałek, 28, październik 2013 09:00
Rafał Rudka

O większości trojanów bankowych zazwyczaj dowiadujemy się przypadkiem (lub gdy jest już za późno), a później ślad po nich ginie. Istnieją jednak cztery szkodliwe programy z tej kategorii, które po prostu nie chcą umrzeć: Carberp, Citadel, SpyEye, a w szczególności ZeuS. Eksperci z Kaspersky Lab przygotowali zestawienie najważniejszych faktów na temat tych zagrożeń.

Carberp

Pierwotna wersja Carberpa była klasycznym trojanem. Szkodnik ten powstał, by kraść wrażliwe informacje użytkowników, takie jak dane logowania do serwisów bankowych i innych ważnych serwisów online. Skradzione informacje były przekazywane do serwera kontrolowanego przez cyberprzestępców. Prosto i skutecznie. Twórcy tego trojana poszli jednak o krok dalej i wykorzystali technologię rootkit, by szkodnik mógł jak najdłużej pozostać niezauważony w zainfekowanym systemie.

Kolejna generacja Carberpa przyniosła nowy zestaw wtyczek - jedna z nich usuwała z systemu oprogramowanie antywirusowe, kolejna dezaktywowała inne szkodliwe programy, jeżeli były obecne (swego rodzaju konkurencja między cyberprzestępcami). Sytuacja zrobiła się jeszcze bardziej niebezpieczna, gdy cyberprzestępcy uzbroili Carberpa w umiejętność szyfrowania skradzionych danych, w wyniku czego mogły one niezauważone przepływać między zainfekowanymi komputerami a serwerami przestępców. Zdaniem badaczy Carberp był pierwszym szkodliwym programem, którego twórcy wykorzystali losowo generowany szyfr kryptograficzny zamiast klucza statycznego.

W swojej kolejnej ewolucji Carberp zaczął wykorzystywać niesławny pakiet exploitów Blackhole, co - dzięki wykorzystaniu wielu luk w zabezpieczeniach popularnych aplikacji - spowodowało nagły wzrost liczby infekcji. Twórcy Carberpa byli na fali. Udało im się nawet stworzyć szkodliwy moduł dla Facebooka, który nakłaniał użytkowników do podawania różnych informacji finansowych.

Od tego momentu sytuacja cyberprzestępców stojących za Carberpem zaczęła się pogarszać. Rosyjskie władze schwytały osiem osób, co do których istniały podejrzenia, że są zamieszane w korzystanie z tego szkodliwego programu. Wkrótce po tym nastąpiły kolejne aresztowania. Doszło nawet do sytuacji, w której twórcy Carberpa żądali 40 000 dolarów za możliwość "wynajęcia" trojana. Wszystko to skończyło się, gdy w ubiegłym roku kod źródłowy tego szkodliwego programu został opublikowany w internecie, co dało do niego dostęp niemal każdemu.

Citadel

Citadel to wariacja na temat króla szkodników finansowych - ZeuSa. Pojawił się w 2011 r. wraz z szeregiem innych szkodliwych programów, tuż po tym, jak kod źródłowy ZeuSa trafił do internetu. Grupa (lub grupy) cyberprzestępców stojących za Citadelem stworzyła społeczność klientów i współpracowników na całym świecie, którzy byli zainteresowani korzystaniem z tego narzędzia i nieustannym rozwijaniem go. Do najbardziej interesujących możliwości dodanych do Citadela należy szyfrowanie własnych plików konfiguracyjnych i całej komunikacji z serwerem kontrolowanym przez cyberprzestępców, umiejętność unikania wykrywania, zdolność do blokowania dostępu do stron związanych z bezpieczeństwem internetowym oraz nagrywanie użytkowników przy użyciu kamer podłączonych do zainfekowanych komputerów.

Sieć współpracowników działających nad rozwojem Citadela nie ustawała w dodawaniu nowych funkcji, czyniąc go coraz bardziej skutecznym narzędziem do kradzieży danych finansowych i wszelkich innych

wrażliwych informacji. Wszystko układało się po myśli cyberprzestępców, aż do momentu, gdy Microsoft wraz z kilkoma innymi firmami przeprowadził operację, której efektem było wyleczenie niemal 90% komputerów zainfekowanych Citadelem.

SpyEye

SpyEye miał być trojanem, który będzie w stanie rywalizować z ZeuSem. Miał potencjał, było o nim głośno, ale ostatecznie nie udało się - ZeuS pozostał królem trojanów bankowych. Nie zmienia to jednak faktu, że SpyEye sporo namieszał. W pewnym momencie doszło nawet do sytuacji, w której SpyEye i ZeuS połączyły siły, by utworzyć mega-botnet, którego zadaniem była kradzież informacji bankowych na ogromną skalę. Twórcom SpyEye'a udało się przeprowadzić skuteczny atak na stronę billingową operatora mobilnego Verizon, w wyniku czego doszło do kradzieży wielu danych osobistych i finansowych. Minął cały tydzień, zanim operatorzy serwisu zauważyli, że dzieje się coś niedobrego! SpyEye pojawił się także w sklepie Amazon oraz na urządzeniach z Androidem, jednak seria aresztowań i w pewnym zakresie brak efektywności zakończyły żywot tego trojana.

Latem 2012 r. trzech mężczyzn zostało aresztowanych za korzystanie ze SpyEye'a do przeprowadzenia zorganizowanej operacji kradzieży informacji finansowych. W maju br. schwytany został domniemany twórca SpyEye, któremu po ekstradycji do Stanów Zjednoczonych przedstawiono ponad trzydzieści zarzutów związanych z oszustwami bankowymi i tworzeniem sieci zainfekowanych komputerów. Od tego czasu nie słyszeliśmy zbyt wiele nowych doniesień o trojanie SpyEye.

ZeuS

Ten nazwany imieniem króla greckich bogów trojan bankowy jest niezrównany pod względem zasięgu, efektywności i użytych technik kradzieży danych. Ze względu na to, że w 2011 r. kod źródłowy ZeuSa został publicznie udostępniony, obecnie niemal każdy trojan bankowy posiada jakieś jego elementy. O tym, jak powstawał i jakie możliwości posiada ZeuS, można by napisać całą powieść, dlatego w tym zestawieniu przedstawione zostaną tylko najważniejsze informacje.

O ZeuSie zrobiło się głośno w 2007 r., gdy został wykorzystany do kradzieży danych uwierzytelniających z Ministerstwa Transportu Stanów Zjednoczonych. Od tego czasu szkodnik ten zainfekował dziesiątki milionów komputerów i umożliwił kontrolującym go cyberprzestępcom kradzież setek milionów dolarów. Wszystko trwało do 2011 r., kiedy twórcy ZeuSa ogłosili, że kończą działalność, i opublikowali kod źródłowy swojego "dzieła" w internecie. W więzieniach na całym świecie siedzą setki przestępców zaangażowanych w oszustwa finansowe z udziałem ZeuSa.

Co ciekawe, ZeuS był jednym z pierwszych szkodliwych programów sprzedawanych tak jak legalne aplikacje - twórcy dystrybuowali licencje. Do momentu, w którym jego kod stał się publiczny, szkodnik ten był prawdziwą zmorą banków i innych instytucji finansowych, a lista jego ofiar jest bardzo długa i obejmuje największe banki na świecie, korporacje oraz organizacje rządowe.

ZeuS jest także znany z tego, że wykorzystywał swojego mobilnego "młodszego brata" - ZitMo - w celu obchodzenia uwierzytelniania dwuskładnikowego wykorzystywanego przez banki do autoryzowania transakcji online poprzez kody jednorazowe wysyłane w wiadomościach SMS.

Ochrona

Wymienione powyżej trojany bankowe mają kilka cech wspólnych: próbują uniknąć wykrycia przez oprogramowanie antywirusowe, przechwytują znaki wprowadzane z klawiatury, kradną dane z przeglądarek internetowych i plików na dysku oraz wszystkie informacje, które mogą pomóc cyberprzestępcom włamać się do kont bankowych i serwisów finansowych online. Trojany te mogą nawet instalować mobilne szkodliwe programy na smartfonach, by przechwytywać kody jednorazowe wysyłane przez banki w SMS-ach. Spośród wszystkich szkodliwych programów trojany bankowe stanowią największe zagrożenie dla finansów użytkowników. Właśnie dlatego ochrona przed nimi musi stanowić ważny element oprogramowania bezpieczeństwa.

Kaspersky Lab zadbał o to, wprowadzając unikatową technologię "Bezpieczne pieniądze", która wbudowana jest w ich niektóre programy.

Źródło: Kaspersky Lab Polska