

# Hakerzy wracają do źródeł?

Autor: Serchio  
05.02.2010.

## G-DATA

Złośliwe oprogramowanie jest dziś używane w szczególności do kradzieży danych oraz popełniania przestępstw finansowych. Wzmożona aktywność cyberprzestępców pod koniec 2009 roku, w kontekście takich wydarzeń, jak ataki na klientów iPKO oraz WBK, zwróciła uwagę mediów na coraz bardziej popularne zjawisko phishingu. Wydaje się jednak, że na początku 2010 roku wirtualni włamywacze zmienili kierunek działań. Dziś ich celem jest stworzenie polimorficznego zagrożenia, które będzie w stanie obejść mechanizmy wykrywania antywirusa.

Dzisiejsza sytuacja na czarnym rynku przypomina tą sprzed kilkunastu lat. Według instytucji monitorujących incydenty w sieci, mamy do czynienia z wirtualną wojną gangów, podczas której złośliwe oprogramowanie tworzy się po to, by udowodnić swoje umiejętności, czy wykraść informacje członkom konkurencyjnego cybergangu. W ślad za tym twórcy złośliwego oprogramowania skupiają swe działania na tworzeniu skażonych kodów, które ulegając rekompilacji co kilka minut, będą w stanie obejść najbardziej zaawansowane mechanizmy bezpieczeństwa. Problem polega na tym, że skażonego kodu nie sposób kontrolować, a niebezpieczne pliki często atakują również systemy standardowych użytkowników sieci.

Twórcy złośliwego oprogramowania mają repertuar narzędzi, który umożliwia im zbadanie skuteczności własnego wirusa. Największy powodzeniem już od dłuższego czasu cieszą się tak zwane multiskanery działające w trybie online, jak np. popularny Virus Total. Mechanizm wykrywania tego typu aplikacji opiera się o rozwiązania dostarczane przez wielu producentów programowania antywirusowego. Tego typu test powala na sprawdzenie, czy skażony plik jest w stanie ukryć się również przed skanerami działającymi w technologii cloud computing, które wykrywają zagrożenie na podstawie analizy wektorów infekcji. Równie cennych informacji dostarczają testy dynamiczne &ndash; infekując system za pomocą zbioru wyselekcjonowanych próbek można rozpoznać, w którym momencie złośliwe oprogramowanie jest wykrywane przez mechanizmy ochrony. Jeżeli nastąpi to dopiero wtedy, gdy zainfekowany plik przedostanie się do sieci lokalnej, a antywirus nie usunął archiwum zawierającego wirusy, to z dużym prawdopodobieństwem można stwierdzić, że bezpieczeństwo całego systemu stoi pod znakiem zapytania.

Polimorficzne zagrożenia to szczególnie typ złośliwego oprogramowanie, które w dzisiejszych czasach stanowią największe niebezpieczeństwo dla użytkowników Internetu. Wykorzystywane w tym celu trojany dostają się do systemu za pomocą ataków typu drive &ndash; by download, a więc takich, które mogą przebiegać bez wiedzy ofiary. &bdquo;Największe zagrożenie stanowią tu skompresowane pliki zawierające próbki Trojanów, których proces instalacji składa się z kilkunastu etapów. W przypadku tak skonstruowanego zagrożenia ciężko jest przewidzieć potencjalny mechanizm infekcji systemu.

Zainstalowany w ten sposób Trojan, umożliwia następnie pobranie innego złośliwego oprogramowania, takiego jak np. spyware czy keyloggery, które z dużym prawdopodobieństwem nie będzie rozpoznane przez mechanizm bezpieczeństwa&rdquo; tłumaczy Tomasz Zamarlik z G Data Software.

Zainstalowane oprogramowanie jest trudne do zidentyfikowania. Jeżeli komputer użytkownika nie jest chroniony zaporą firewall, to o aktywności zainfekowanego pliku Internauta może dowiedzieć się jedynie śledząc nietypowe obciążenie procesora. Taka analiza wymaga jednak wiedzy specjalistycznej, którą posiada niewielki odsetek użytkowników Internetu. W tym przypadku idealny model zabezpieczenia komputera zapewnia jedynie połączenie mechanizmów ochrony lokalnej z rozwiązaniami technologii cloud, lecz tego typu system nie jest jak na razie popularnym rozwiązaniem na rynku antywirusów. Proaktywny system ochrony powinien zadziałać jeszcze przed pobraniem złośliwego oprogramowania, identyfikując go na podstawie samej analizy prawdopodobnych wektorów infekcji. Jeżeli system antywirusa opiera się tylko na jednym z mechanizmów ochrony, to skuteczność wykrywania spada o kilkanaście procent.

Jak zauważają eksperci z G Data Software, trudno jest oszacować, na ile problem polimorficznych zagrożeń stanowi zagrożenie dla polskich Internautów. Nie zmienia to jednak faktu, że w podsumowaniu za 2009 rok odnotowano znaczący wzrost aktywności szkodliwych plików, które dostawały się na komputer ofiary za pomocą popularnych form ataków. Cyberprzestępcy odchodzą od phisingu, mając na uwadze rosnącą świadomość Internautów dotyczącą tego typu ataków. Z tego powodu, dziś szczególnie popularne są infekcje oparte na mechanizmie drive &ndash; by download, które przebiegają w sposób całkowicie niewidoczny dla użytkowników sieci.