

W tym roku firma G Data Software, znany producent oprogramowania antywirusowego, obchodzi 25 -lecie istnienia. Tak długa obecność na rynku systemów zabezpieczających zaowocowała nadaniem marce wyróżnienia „Jakość Roku 2009”. O zmianach, jakie na przestrzeni tego okresu udało się zaobserwować na rynku online rozmawiamy z Tomaszem Zamarlik, marketing managerem G Data Software.

Niemal każdego dnia media informują nas o nowych zagrożeniach, jakie zostały wykryte w sieci. Kilka dni temu głośnym echem odbiła się informacja o niespotykanej dotąd skali proliferacji Trojana Zeus, któremu udało się zainfekować ponad 75 tysięcy komputerów. Co obecnie według Pana stanowi dziś największe zagrożenie dla użytkowników sieci?

Myślę, że można tu wskazać dwa czynniki – po pierwsze brak ostrożności wśród internautów, po drugie innych użytkowników sieci [śmiech]. Okazuje się, że najsłabszym ogniwem w systemie zabezpieczeń jest bagatelizowanie problemu oraz brak dbałości na przykład o częste aktualizowanie baz sygnatur. Jeżeli chodzi o typowe malware, to obecnie największym wyzwaniem dla branży antywirusowej są rootkity - narzędzie pomocne w dokonywaniu włamań do systemów informatycznych. Jak wynika również z naszych obserwacji stale rośnie liczba spamu, masowo wysyłanego zarówno do użytkowników domowych, jak i administratorów firmowych sieci. Konsekwencje mogą być różne – począwszy od kilku utraconych plików i wiadomości e-mail, skończywszy na zniszczeniu zawartości dysków. Od początku roku zaobserwować można również powrót do trendów znanych nam z lat 90, kiedy to celem było zniszczenie komputera, lub danych zapisanych na dyskach, by w ten sposób utrudnić pracę użytkownikowi.

Na czym polega zmiana zachowań w środowisku hakerów? Co było ich celem kiedyś, a co jest nim teraz?

Dziś słowo haker nie odpowiada definicji znanej nam sprzed kilku lat. Wyłoniła się natomiast nowa grupa cyberprzestępców, którzy dokonują ataków na indywidualnych użytkowników Internetu, czy też systemy firmowe, w celu odniesienia konkretnych korzyści materialnych. Malware jest dziś wykorzystywane do kradzieży poufnych danych, lub przejęcia kontroli nad komputerem, który można wykorzystać do kolejnych ataków. Zmianie uległ również rodzaj wykorzystywanych narzędzi – kilka lat temu największe zagrożenie stanowiły wirusy, dziś niebezpieczeństwo czyha na użytkowników portali społecznościowych, klientów e-banków, konsumentów sklepów online. Ataki na Internautów mają bardziej komercyjny charakter, natomiast cyberprzestępcy wykorzystują w tym celu najnowsze generacje zagrożeń, jak na przykład rootkity, czy spyware. Wykorzystywane są również techniki marketingowe, które obniżają koszty ponoszone przez przestępców i znacznie podnoszą skuteczność ich działań. Zmieniło się prawie wszystko, od ideologii po komercjalizację tak szybko można byłoby to opisać.

Który element stanowi najsłabsze ogniwo w systemie bezpieczeństwa? Co należałoby zmienić, by w polskiej sieci zmalała liczba ataków?

Wbrew pozorom najsłabszy element jest nasza wiedza, mawia się że najsłabszym ogniwem każdego systemu zabezpieczeń jest człowiek. Chociaż wciąż mówi się o zagrożeniach występujących w Internecie, to jednak nadal wiemy niewiele. Największym problemem jest komercjalizacja, która przebiega często kosztem uczciwości. Wyraźnie widać to w niektórych mediach, które nie edukują, lecz stawiają na skandal. Sprawę pogarsza fakt, że cyberprzestępczość, stała się teraz opłacalnym biznesem. Co więcej, ofiarą działań może być niemal każdy użytkownik Internetu – osoba kupująca w wirtualnym sklepie, logująca się na stronę banku, jak również pracownik firmy przechowujący na dyskach swojego komputera poufne informacje. Dlatego G Data Software już od dłuższego czasu podejmuje dyskusje na takie tematy, jak faktyczna skuteczność programów antywirusowych, nowe rodzaje zagrożeń, najlepsze formy ochrony przed atakami.

Równie źle przedstawia się sytuacja, jeżeli chodzi o dbałość i systematyczność Internautów. Bardzo rzadko użytkownicy wirusów aktualizują bazy sygnatur wirusów czy same programy, w których wykryto niedociągnięcia programistyczne. Wydawać się może że są to drobne zaniedbania jednak właśnie one mogą prowadzić do tego, że nawet bardzo wydajny antywirus może okazać się nieskuteczny.

Jakie rozwiązania okażą się najbardziej skuteczne dla użytkowników sieci? W jaki rodzaj ochrony najlepiej inwestować?

W przypadku firm wdrażane mechanizmy bezpieczeństwa powinny obsługiwać sieci o charakterze heterogenicznym, natomiast cechą charakteryzującą rozwiązania przeznaczone dla użytkowników domowych jest kompleksowość ochrony. Proponowane rozwiązania są bardzo różnorodne i dedykowane do sprecyzowanych segmentów rynku. Obecnie najlepszą ochronę dają tak zwane pakiety zabezpieczające typu Internet Security, które zapewniają kompleksową ochronę przed polimorficznymi zagrożeniami. Zawierają one zwykle programy antywirusowe, zapory sieciowe, dodatkowe moduły chroniące przed różnorodnym złośliwym oprogramowaniem, moduły antyspamowe oraz filtr kontroli rodzicielskiej. Pakiety pozwalają na zapewnienie użytkownikom wszechstronnej ochrony, również w czasie rzeczywistym. Nie należy także zapominać o aktualizacjach programów, jakie tworzone są przez komórki laboratoryjne, zajmujące się zbieraniem informacji o najnowszych zagrożeniach, które pojawiają się w sieci.

W jaki sposób realizowane są przez G Data Software działania edukacyjne, o których wcześniej była mowa?

Takie działania realizowane są na dwa sposoby – po pierwsze poprzez informowanie o nowych zagrożeniach, po drugie wydając obszernie raporty na temat poziomu bezpieczeństwa Internetu. Dążymy do tego, by zwiększyć wiedzę użytkowników sieci na temat nowych zagrożeń oraz pokazać, w jaki sposób najlepiej bronić się przed infekcją. Takie działania są tym bardziej istotne, że wielu cyberprzestępców korzysta z trudnych do wykrycia form ataku. Przykładem jest np. zagnieżdżanie niebezpiecznych kodów w formie pliku JavaScript na popularnych serwisach www. W tym przypadku internauta nie musi pobierać ze strony żadnych dokumentów – wystarczy, że otworzy stronę w niezaktualizowanej przeglądarce.

G Data Software