

Oszustwa ukryte
głęboko w chmurach
Przenoszenie aplikacji do
sieci zwiększa liczbę zagro-
żeń bezpieczeństwa. **►IV**

Oszustwa ukryte głęboko w chmurach

INTERNET | Przenoszenie aplikacji do sieci zwiększa liczbę zagrożeń bezpieczeństwa

TOMASZ BOGUSZEWICZ

Aż 65 proc. spośród przebadanych po obu stronach Atlantyku internautów obawia się, że korzystanie z serwisów społecznościowych nie jest bezpieczne – wynika z badania przeprowadzonego przez ame-

rykańską firmę EMC. Aż 81 proc. respondentów uważa, że ich osobiste informacje, które sami zamieszczają w takich serwisach jak Facebook, nie są dobrze chronione.

Nie bez powodu. – Dzięki ogromnemu zasięgowi serwisów społecznościowych to raj dla przestępców internetowych, szcze-

gólnie tych zajmujących się kradzieżą danych osobowych – mówi Christopher Young, wiceprezes RSA.

Analitycy firmy wskazują na coraz bardziej wyrafinowane socjotechniczne sposoby usypiania czujności użytkowników. Dobrą okazją dla cyberprzestępców są np. głośne wydarzenia

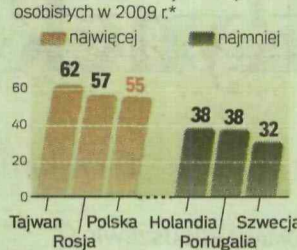
medialne, jak choćby ubiegłoroczna śmierć Michaela Jacksona czy skandal rodzinny golfisty Tigera Woodsa. Wiele pozornie spontanicznie zamieszczanych informacji zawiera linki do zewnętrznych stron, w tym zawierających złośliwy kod.

– Przestępcy miewają w przygotowaniu różne formy ataków,

Rodzaje zagrożeń występujących w sieci w 2009 r., w proc. w ujęciu globalnym



Odsetek zainfekowanych komputerów osobistych w 2009 r.*



*dane pozyskane za pomocą skanera online ActiveScan 2.0, źródło: Panda Security

GDZIE I CZYM NAJĘTWIEJ ZAINFEKOWAĆ KOMPUTER

które uruchamiają w momencie pojawienia się ważnych wydarzeń. W takich przypadkach ludzie są bardziej skłonni do odwiedzania zainfekowanych serwisów internetowych. Wśród nich zdarzają się całkowicie fałszywe witryny, udające np. znane serwisy informacyjne – wyjaśnia Christopher Young. Facebooka i Twittera do rozpowszechniania wykorzystywał niedawno m.in. wirus Koobface.

Metoda na fałszywki

Jeszcze bardziej wyrafinowaną, coraz bardziej rozpowszechnioną metodą dystrybucji zagrożeń jest tzw. scareware, czyli fałszywe oprogramowanie antywirusowe. Programy tego typu oferowane są w sieci za darmo, obiecując użytkownikowi ochronę przed zagrożeniami. W rzeczywistości same infekują komputer, najczęściej zamieniając go w element tzw. botnetu, wykorzystywanego do masowego rozsyłania spamu. Jak szacuje firma McAfee, amerykański producent zabezpieczeń, programy typu scareware trafiają każdego dnia na ok. milion komputerów na całym świecie. – Liczba tego typu zagrożeń w ciągu dwóch ostatnich lat wzrosła o 660 proc. – twierdzi Francois Paget, ekspert McAfee Labs.

Internetowi przestępcy fałszują jednak nie tylko oprogramowanie antywirusowe, ale także znajdujące się do niedawna poza podejrzeniem tzw. wtyczki (plug-ins), czyli mini-programy rozszerzające funkcjonalność popularnych programów. Mozilla Foundation, rozwijająca darmową przeglądarkę Firefox, poinformowała niedawno o stworzonej przez jednego z internautów fałszywej wtyczce, mogącej śledzić hasła

wpisywane do internetowych formularzy.

Sieci bardziej zagrożone

Jak zauważa Rafał Wolsztyński, inżynier systemowy w firmie informatycznej ITelligence, nowym sposobem rozprawiania zagrożeń sprzyja cloud computing, czyli dominujący od kilku lat w informatyce trend polegający na przenoszeniu nie tylko informacji, ale także aplikacji do sieci. Przechowywanie danych w "chmurze" i wynajem aplikacji pozwala na oszczędności, ale stwarza też nowe zagrożenia.

– Posiadające wielostopniowe zabezpieczenia sieci lokalne zapewniały lepszą ochronę informacji. Ataki obliczone na zdobycie informacji zostaną przekierowane na serwery. Nie spodziewam się zmniejszenia liczby zagrożeń w najbliższej przyszłości – uważa Wolsztyński. Według niego powstanie nowych zagrożeń może się wiązać np. z dopuszczonym niedawno stosowaniem lokalnych znaków w nazwach witryn internetowych. – Stwarza to nowe możliwości wyłudzenia danych, bazując na podobieństwie znaków w nazwach witryn – dodaje Wolsztyński.

Przeniesienie zasobów w internetową chmurę sprawia, że wiele firm staje przed wyzwaniem skonstruowania zupełnie nowej polityki bezpieczeństwa IT. – Najważniejszym wyzwaniem jest filtrowanie ruchu sieciowego i poczty elektronicznej. Trzeba jednak pamiętać, że pojawienie się "chmury" nie eliminuje zagrożeń pochodzących z wnętrza infrastruktury w firmach – zaznacza Gaweł Mikołajczyk, ekspert ds. bezpieczeństwa firmy Cisco. ■

@masz pytanie, wyślij e-mail do autora t.boguszewicz@rp.pl

POWIEDZIAŁ

„RZECZPOSPOLITEJ”



DARIUSZ WÓJCIK | BUSINESS SOLUTION MANAGER, COMARCH SA

Głównym sposobem rozpowszechniania malware w najbliższym czasie będzie wciąż umieszczanie go na stronach WWW. To najskuteczniejsza i najtańsza metoda umożliwiająca infekcje na masową skalę, przed którą obrona jest trudna i kosztowna – wymaga bowiem analizy w warstwie aplikacyjnej. Pewną nowością jest dopasowanie złośliwego oprogramowania do profilu użytkownika. W szczególnych przypadkach, kiedy celem ataku są komputery konkretnych osób, np. kluczowych pracowników dużych firm mających dostęp do ważnych informacji, atak jest przygotowywany indywidualnie. W takiej sytuacji ofiara praktycznie nie ma szans uniknięcia błędu. Popularnym sposobem rozpowszechniania infekcji jest także zagnieżdżanie złośliwego kodu, np. w aplikacjach często pobieranych z Internetu. W ten sposób zainfekowaną nielegalną kopię systemu Microsoft Windows 7 ściągnęło kilkadziesiąt tysięcy internautów. tbo