10 prognoz zagrożeń

Laboratorium TrendLabs firmy Trend Micro pracowało zestaw dziesięciu największych zagrożeń czyhających na nas w 2009 roku, tych nowych i tych już nazbyt dobrze

1. Bolączki Web 2.0
Korzyści (i zagrożenia) płynące ze stosowania aplikacji Web 2.0 będą w 2009 roku nadal aktualne. Hakerzy będą korzystać z technik tworzenia struktur przypominających zwykły kod, takich jak IFRAMES, będą też nadal wykorzystywać przeglądarki i inne aplikacje internetowe jako nośniki infekcji. Wprowadzenie przeglądarki Google Chrome, zbliżające się oficjalne udostępnienie przeglądarki Internet Explorer 8 oraz wzrost popularności aplikacji typu „przeglądarka jako platforma" pociągnie za sobą rozwój nowych rodzajów ataków.

2. Alternatywne systemy operacyjne
Wszystko, co dobre, szybko się kończy — w tym rzekome bezpieczeństwo platform alternatywnych. Zagrożenia wynikające z wykorzystania błędów w alternatywnych systemach operacyjnych będą coraz powszechniejsze, zwłaszcza w obliczu rosnącej popularności systemów Mac i Linux.

3. Microsoft — stały cel
Ulubionym obiektem ataków twórców szkodliwego oprogramowania jest Microsoft i nie zanosi się na to, aby rok 2009 miał tu przynieść zmiany. W związku z udostępnieniem systemu Windows 7 należy spodziewać się ataków przestępców cybernetycznych, którzy z pewnością potraktują zapowiedzi o całkowitej odporności nowego systemu na wirusy jako wyzwanie. Na podobne ataki testujące poprawność opracowania będą też narażone projekty Microsoft Surface, Silverlight i Azure.

4. Rozkwit socjotechniki
Cybernetyczni przestępcy będą nadal używać głośnych wydarzeń oraz postaci ze świata showbiznesu i polityki jako przynęty w atakach opartych na socjotechnice. Użytkownicy oczekujący na publikację gier Starcraft 2 i WoW: Wrath of the Lich King również powinni mieć się na baczności. W związku z globalnym kryzysem finansowym będą zdarzać się próby nieuczciwego wykorzystania skłonności konsumentów do oszczędzania, takie jak wiadomości e-mail na tematy ekonomiczne, fałszywe kupony internetowe, fikcyjne propozycje pracy zdalnej i inne.

5. Wojny gangów cybernetycznych
Analitycy zajmujący się dziedziną zabezpieczeń zapowiadają wojny wirusów, robaków i botnetów jako skutek coraz bardziej zaciętej walki o zyski z wyłudzania danych osobowych i oszustw, jak również zmniejszania się gangów cybernetycznych i coraz lepszych zabezpieczeń. Będzie trwała rywalizacja między przestępcami z krajów Europy Środkowej i Chin o pierwszeństwo we wprowadzaniu najnowszych eksploitów w zestawach szkodliwego oprogramowania.

6. Rosnące zagrożenia w świecie wirtualnym
Wiele zagrożeń znanych dotąd ze świata rzeczywistego pojawia się również w świecie wirtualnym. Cybernetyczni przestępcy szukają publiczności dla swoich wyczynów, dlatego ich ofiarą padają często użytkownicy światów wirtualnych i gracze internetowi. Zagrożenia obecne w światach wirtualnych obejmują całą skalę różnorodnych zachowań użytkowników, czasem nieszkodliwych, jak udostępnianie haseł partnerom, czasem wyrafinowanych, jak oszustwa związane z własnością nieruchomości, a czasem tak groźnych jak polowania gangów na nowych użytkowników.

7. Zagrożenia w systemie DNS
Cybernetyczni przestępcy będą wykorzystywać do swoich celów znane luki w rejestrach systemu nazw domen (domain name system — DNS). Według specjalistów używane są już zatrute pamięci podręczne DNS, które pozwalają tworzyć ukryte kanały komunikacyjne, obchodzić zabezpieczenia i dostarczać szkodliwe treści. Mimo że dostawcy zabezpieczeń ściśle współpracują z organizacjami zarządzającymi rejestrami DNS, konieczne jest zaangażowanie w ten problem Internetowej Korporacji ds. Nadawania Nazw i Numerów (Internet Corporation for Assigned Names and Numbers — ICANN).

8. Rozkwit nielegalnych interesów
Cybernetyczne przestępstwa to już cały przemysł i niestety w roku 2009 będzie się on dalej rozwijać. Szkodliwe oprogramowanie do kradzieży informacji, ukierunkowane na dane logowania oraz informacje z systemów bankowych i dotyczące kart kredytowych będzie nadal bardzo popularne.

9. Rozwój inteligentnego szkodliwego oprogramowania
Rozwój szkodliwych technologii jest nieunikniony, ponieważ twórcy złośliwych kodów wciąż opracowują i wprowadzają w obieg oprogramowanie, które ma być niewykrywalne i dzięki temu niemożliwe do usunięcia. Należy oczekiwać pojawiania się kolejnych rodzin szkodliwego oprogramowania w ograniczonej liczbie wariantów, przez co stojące przed producentami rozwiązań antywirusowych zadanie tworzenia modeli heurystycznych umożliwiających ich wykrywanie, będzie coraz trudniejsze.

10. Odsiecz na horyzoncie
Nie wszystkie nowiny nastrajają pesymistycznie. Działania społecznościowe zaczynają coraz częściej skutkować unieszkodliwieniem nośników zagrożenia. W miarę jak narasta zniecierpliwienie tupetem cybernetycznych przestępców i ich atakami, działania społeczności będą coraz częściej prowadzić do demaskowania czarnych charakterów, tak jak w przypadku firm Atrivo/Intercage i McColo w roku 2008. ■