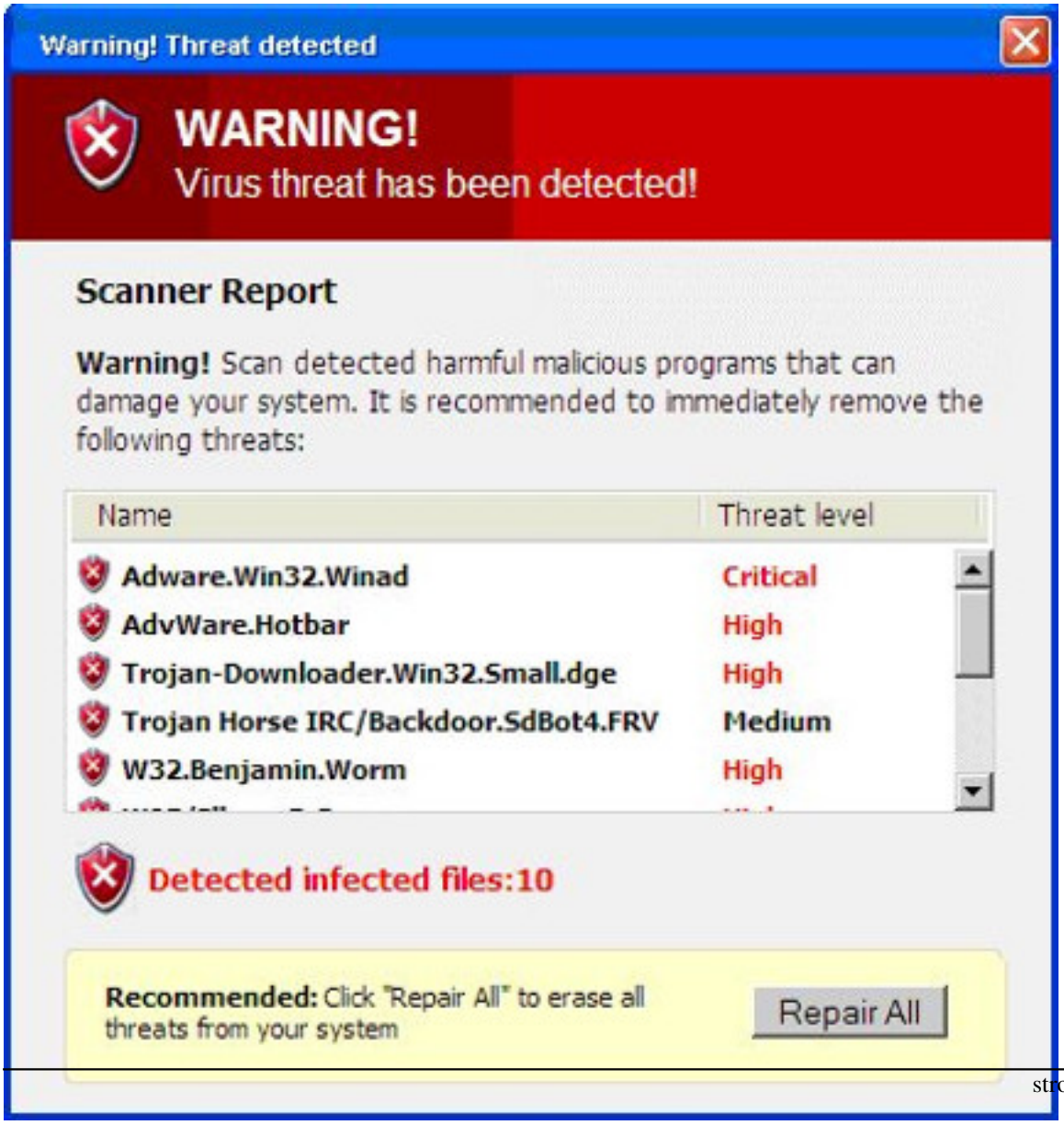
Według najnowszego raportu Google, fałszywe antywirusy stanowią już 15% złośliwego oprogramowania w Sieci. To oznacza aż sześciokrotny przyrost w porównaniu z rokiem 2009.

Od początku 2009 do lutego 2010 skanery Google przeanalizowały 240 milionów stron internetowych. Jedenaście tysięcy zbadanych stron zawierało tzw. "**scareware**", czyli fałszywe oprogramowanie antywirusowe - czytamy w raporcie Google "The Nocebo Effect on the Web: An Analysis of Fake Anti-Virus Distribution". Gwałtowny wzrost ilości "scareware" w Sieci dowodzi, że cyberprzestępcy coraz częściej posługują się technikami inżynierii społecznej.

„Nasze obserwacje potwierdzają wnioski, do których doszło w swoim raporcie Google" – mówi Tomasz Zamarlik, Marketing Manager z firmy **G Data Software**. "Nastąpił radykalny wzrost ilości scareware w Sieci. Oszuści liczą, że jeśli przestraszą internautę fałszywym alarmem o zagrożeniu, ten natychmiast kupi - z wdzięcznością! - lekarstwo na wirusa. Wiele osób przekazuje w takich okolicznościach numer swojej karty kredytowej przestępcom i pada ofiarą kradzieży. Mowa tu o kwotach znacznie przekraczających wartość legalnego, sprawdzonego na rynku oprogramowania. Problem jest tym bardziej uciążliwy, że może dotyczyć praktycznie każdej strony internetowej - w roku 2009 padli jego ofiarą czytelnicy New York Times!”.



Jak to działa
Ofiarą przestępstwa, o którym mowa w raporcie Google, może być każdy internauta surfujący po Internecie. Na jego ekranie pojawia się nagle powiadomienie, do złudzenia przypominające okna komunikatów systemowych. Z treści dowiaduje się, iż jego komputer nie jest dostatecznie chroniony przed złośliwym oprogramowaniem z Sieci. Otrzymuje propozycję zakupu programu antywirusowego. Jeśli z niej skorzysta, umożliwia cyberprzestępcy dostęp do danych na swoim komputerze. Mechanizm działania skryptu jest tak zaawansowany, że wykrywa wersję systemu na komputerze użytkownika i na tej podstawie wyświetla właściwe okno.

Legalne oprogramowanie antywirusowe jest w stanie poradzić sobie ze szkodami wyrządzonymi przez swoje "złośliwe podróbki", tylko jeśli jest stale aktualizowane. Fałszywe antywirusy wciąż ewoluują. Stają się coraz trudniejsze trudne do wykrycia, a nawet jeśli zostaną wykryte, ich odinstalowanie nie jest rzeczą łatwą. Uniemożliwiają instalację aktualizacji systemu, jak również nie dopuszczają do instalacji bezpiecznego oprogramowania antywirusowego.

Liczy się ilość
Domeny mają teraz krótszą żywotność niż jeszcze rok temu, ale za to mnożą się w nieskończoność (Google odnotowało wzrost ich liczby o około 600% od stycznia 2009 r.). W raporcie Google czytamy, że choć łączna liczba podobnych domen wzrosła, to zmniejszył się średni czas ich żywotności: w kwietniu 2009 było to 100 godzin, we wrześniu 2009 około 10 godzin. W styczniu roku 2010 długość życia "złośliwej strony" wynosiła zaledwie jedną godzinę.

Popularne przeglądarki, takie jak Google Chrome czy Firefox, są wyposażone w opcję „safe browsing”, która ostrzega internautów przed niebezpiecznymi stronami. Jednak krótka żywotność w połączeniu z rosnącą ilością tych domen sprawiają, że przeglądarki nie radzą sobie z wyławianiem ich spośród stron bezpiecznych. Statystyki wykrywania fałszywych antywirusów w ostatnim roku poważnie zmalały i według Google wynoszą teraz mniej niż 20%.

Pomiędzy specjalistami do spraw bezpieczeństwa IT a cyberprzestępcami, toczy się nieustanna walka. Dziś - bardziej niż kiedykolwiek - liczy się w niej czas. Niels Provos, jeden z autorów raportu Google, stwierdza: „Doszliśmy do wniosku, że nawet jeśli masz na komputerze program antywirusowy, ale baza sygnatur zagrożeń jest przeterminowana choćby tylko o kilka dni, to Twoje szanse ochrony maleją w drastycznym stopniu.”

Someday Interactive