Co czyha na twój komputer w 2011 r.

Kategoria: Aktualności
Opublikowano: sobota, 29, styczeń 2011 00:00
Odsłony: 2178

Jak czytamy w portalu www.idg.pl, w 2011 roku może nastąpić przełom w postaci zmian w charakterystyce organizacji przestępczych i ich celów. Zdaniem Aleksandra Gostiew, głównego eksperta ds. bezpieczeństwa w Kaspersky Lab, zmiany te będą szły w parze z zanikiem szkodliwego oprogramowania pisanego przez amatorów (których celem było pochwalenie się swoimi zdolnościami pisania wirusów). Głównym źródłem dochodów cyberprzestępców pozostanie kradzież danych uwierzytelniających transakcje bankowe online, spam, ataki DDoS (ang.: distributed denial of service; odmowa usługi), wyłudzenia oraz oszustwa.

Miniony rok był okresem "luk w zabezpieczeniach". "Rok 2011 zapowiada się jeszcze gorzej" - prognozuje A. Gostiew. Wzrost liczby szkodników wykorzystujących błędy programistyczne będzie spowodowany nie tylko wykrywaniem nowych luk w popularnych rozwiązaniach, takich jak produkty firmy Microsoftu, Adobe czy Apple, ale również szybszą reakcją cyberprzestępców na pojawienie się takich luk.

"Co więcej, ulubioną bronią cyberprzestępców w 2011 roku nie będą wyłącznie luki umożliwiające zdalne wykonanie szkodliwego programu. Centralne miejsce zajmą luki pozwalające na eskalację przywilejów, manipulację danymi oraz obejście mechanizmów bezpieczeństwa" - spodziewa się przedstawiciel Kaspersky Lab.

W 2011 roku może pojawić się nowa kategoria programów spyware, których celem będzie kradzież wszystkiego, co popadnie. "Programy te będą gromadziły wszystkie informacje o użytkowniku: dane dotyczące jego lokalizacji, pracy, przyjaciół, przychodów, rodziny, koloru oczu i włosów itd. Nie pogardzą niczym, analizując każdy dokument i każde zdjęcie przechowywane na zainfekowanym komputerze" - przekonuje A. Gostiew.

"Cyberprzestępcy to mistrzowie innowacji. W branży zabezpieczeń trzeba stale spoglądać w przód i opracowywać technologie ograniczające szkody powodowane przez takie innowacje. Problem polega na tym, że my musimy być gotowi przez cały czas, a im do sukcesu wystarcza jedno udane rozwiązanie" - mówi Rik Fergusson, starszy doradca ds. bezpieczeństwa w firmie Trend Micro.

Firmom rozwijającym narzędzia zabezpieczające nie ułatwia pracy fakt, że tradycyjna cyberprzestępczość coraz częściej wkracza na obszary, których do tej pory starała się unikać, czyli ukierunkowane ataki na firmy. Kiedyś ataki ograniczały się do kradzieży pieniędzy od użytkowników czy instytucji bankowych i systemów płatniczych. Teraz technologia wykorzystywana przez cyberprzestępców jest już tak zaawansowana, że umożliwia szpiegostwo przemysłowe, szantaż i wyłudzenia.

Jakich zagrożeń powinniśmy więc spodziewać się w tym roku?

W 2011 roku może nastąpić przełom w postaci zmian w charakterystyce organizacji przestępczych i ich celów. Zdaniem Aleksandra Gostiew, głównego eksperta ds. bezpieczeństwa w Kaspersky Lab, zmiany te będą szły w parze z zanikiem szkodliwego oprogramowania pisanego przez amatorów (których celem było pochwalenie się swoimi zdolnościami pisania wirusów). Głównym źródłem dochodów cyberprzestępców pozostanie kradzież danych uwierzytelniających transakcje bankowe online, spam, ataki DDoS (ang.: distributed denial of service; odmowa usługi), wyłudzenia oraz oszustwa.

Miniony rok był okresem "luk w zabezpieczeniach". "Rok 2011 zapowiada się jeszcze gorzej" - prognozuje A. Gostiew. Wzrost liczby szkodników wykorzystujących błędy programistyczne będzie spowodowany nie tylko wykrywaniem nowych luk w popularnych rozwiązaniach, takich jak produkty firmy Microsoftu, Adobe czy Apple, ale również szybszą reakcją cyberprzestępców na pojawienie się takich luk.

Jeszcze kilka lat temu luki "zero-day" - tj. takie, na które zaraz po wykryciu powstawały tzw. exploity - nie stanowiło poważnego problemu. W 2010 r. stało się to zjawiskiem powszechnym. Niestety wszystko wskazuje na to, że trend ten będzie kontynuowany, a zagrożenia zero-day staną się jeszcze bardziej rozpowszechnione. "Co więcej, ulubioną bronią cyberprzestępców w 2011 roku nie będą wyłącznie luki umożliwiające zdalne wykonanie szkodliwego programu. Centralne miejsce zajmą luki pozwalające na eskalację przywilejów, manipulację danymi oraz obejście mechanizmów bezpieczeństwa" - spodziewa się przedstawiciel Kaspersky Lab.

Czy do ochrony numerów kont, loginów i haseł oraz dokumentów przechowywanych w komórce niezbędny będzie mobilny antywirus?

Nie będzie nadużyciem stwierdzenie, że pod jeszcze większym "ostrzałem" przestępców znajdzie się Windows 7. To tylko kwestia czasu, a w zasadzie - wzrostu liczby użytkowników korzystających z najnowszej wersji systemu Windows. Nie znaczy to jednak, że wciąż najpopularniejszy produkt Microsoftum, czyli Windows XP, przestanie być atrakcyjnym celem - w systemie tym włamywacze wciąż znajdują liczne luki, które skwapliwie wykorzystują. Popularność XP oraz fakt, że każdy użytkownik jest równocześnie administratorem, tylko zwiększają poziom zagrożenia.

W 2011 roku może pojawić się nowa kategoria programów spyware, których celem będzie kradzież wszystkiego, co popadnie. "Programy te będą gromadziły wszystkie informacje o użytkowniku: dane dotyczące jego lokalizacji, pracy, przyjaciół, przychodów, rodziny, koloru oczu i włosów itd. Nie pogardzą niczym, analizując każdy dokument i każde zdjęcie przechowywane na zainfekowanym komputerze" - przekonuje A. Gostiew. Do tego dojdą fałszywe programy antywirusowe - aplikacje tego typu są po prostu zbyt lukratywne, aby cyberprzestępcy mogli z nich zrezygnować.

Wzrośnie również liczba ataków na użytkowników portali społecznościowych. Większość z nich będzie wykorzystywała luki w zabezpieczeniach i będzie przeprowadzona za pośrednictwem przeglądarek internetowych. Grono 500 milionów użytkowników Facebooka stanowi wymarzone środowisko działania dla cyberprzestępców, którzy mogą "ukryć się w tłumie", równocześnie działając na masową skalę. "Portale społecznościowe koncentrują uwagę przestępców, ponieważ ich funkcjonowanie opiera się zaufaniu, jakim darzymy linki, wiadomości czy aplikacje polecane rzekomo przez naszych znajomych. To znacząco ułatwia zadanie sieciowym szajkom" - przekonuje Michał Iwan, dyrektor zarządzający F-Secure Polska.

Nie zapomnimy również o botnetach, zarówno starych, jak i nowych, które pojawią się w miejsce tych zlikwidowanych (np. Bredolaba). Rik Fergusson z Trend Micro podkreśla, że botnety są nadal uniwersalnym narzędziem cyberprzestępców, ponieważ można je wykorzystywać na wiele różnych sposobów: do rozsyłania spamu, dystrybucji szkodliwego oprogramowania, DDoS, kradzieży informacji itd. "Botnety będą dominować w świecie przestępczym przez co najmniej kilka następnych lat" - ocenia ekspert Trend Micro. Ataki DDoS pozostaną też jedną z największych "plag" Internetu.

Kategoria: Aktualności
Opublikowano: sobota, 29, styczeń 2011 00:00
Odsłony: 2178

Michał Iwan zwraca uwagę na problem gwałtownej eksplozji zagrożeń mobilnych, związanej bezpośrednio z szybkim rozwojem funkcjonalności smartfonów. Urządzenia te pełnią dziś rolę minikomputerów, banków zdjęć, komunikatorów, a nawet okienek bankowych. Nic dziwnego, że cyberprzestępcy zdążyli się zorientować, jak bardzo dochodowy to rynek i nauczyli się na nim zarabiać. "Nie chodzi tu wyłącznie o groźne aplikacje wykonujące bez wiedzy użytkownika drogie międzynarodowe połączenia. Atrakcyjnym łupem dla cybeprzestępców są także podsłuchiwane rozmowy, przechwytywane sms-y i maile, informacje o życiu prywatnym, a przede wszystkim dane gromadzone w telefonie" - ostrzega M. Iwan.

Czyżby więc czekała nas wielka mobilna epidemia, której ofiarami padną numery kont, loginy i hasła, dokumenty oraz zdjęcia przechowywane w komórce? Teza ta wydaje się uprawniona, zwłaszcza że potwierdzają ją kolejni eksperci. Smartfony są jeszcze mniejsze, bardziej mobilne i tańsze niż laptopy, posiadają za to porównywalną wydajność procesora i pamięć na dane. "Od czasu pojawienia się iPhone'a i Androida są coraz częściej stosowane w sieci przedsiębiorstw, a poprzez to nieuchronnie napełniane danymi. Wzrost stosowania smartfonów w przedsiębiorstwie sprowokował hakerów do wykorzystywania luk w zabezpieczeniach mobilnych systemów operacyjnych i szukania nowych bram dostępu do sieci przedsiębiorstwa" - mówi Markus Bernhammer z Sophos.

Źródło: www.idg.pl