Prognoza dotycząca cyberzagrożeń na 2012 rok

Autor:
Aleksander Gostiew, ekspert z Kaspersky Lab

Cyberwojny

Rok 2011 zapisał się jako ten, w którym praktycznie wszyscy globalni gracze zasygnalizowali gotowość do rozwoju i stosowania cyberbroni. Masowa histeria wywołana odkryciem robaka Stuxnet w 2010 r. spowodowała, że wiele państw zaczęło traktować wykorzystanie przeciwko nim cyberbroni jako działanie wojenne. Jednak postępując w ten sposób pomijają bardzo istotne aspekty tego rodzaju zagrożenia. Weźmy na przykład Stuxneta. Szkodnik ten stanowił unikatowe zjawisko: został stworzony wyłącznie do wykorzystania w określonym czasie i miejscu. Co więcej, nie istniało łatwo dostępne rozwiązanie militarne, przy pomocy którego można było je pokonać. To dlatego uważamy, że wykorzystywanie cyberbroni, takiej jak Stuxnet, nadal będzie stanowić odosobnione incydenty. Pojawienie się takich zagrożeń będzie uzależnione w głównej mierze od stosunków między określonymi państwami. Aby została stworzona cyberbroń tej klasy, musi istnieć zarówno agresor jak i ofiara. W przypadku agresora, problem musi być tak poważny, aby dalsze ignorowanie go nie było już możliwe, a działania militarne nie wchodziły w grę. Analiza obecnych konfliktów międzypaństwowych może pomóc przewidzieć podobne incydenty w przyszłości.

To wszystko dotyczy cyberbroni w rodzaju robaka Stuxnet, której celem jest przeprowadzanie cybersabotażu. W przeciwieństwie do niej, inne typy cyberbroni, umożliwiające niszczenie danych w określonym czasie, będą prawdopodobnie szeroko rozpowszechnione. Rozwiązania, takie jak “kill switch” (funkcja pozwalająca na błyskawiczne zamknięcie systemu), bomby logiczne itd. mogą być regularnie rozwijane i systematycznie stosowane. Co więcej, tworzenie takich programów może być zlecane prywatnym kontrahentom angażowanym przez wojsko, organy ścigania oraz agencje wywiadowcze. W wielu przypadkach zleceniobiorca nigdy nie pozna tożsamości ostatecznego klienta.

Można założyć, że w 2012 r. główne cyberkonflikty będą dotyczyły tradycyjnych osi konfrontacji: Stany Zjednoczone i Izrael kontra Iran oraz Stany Zjednoczone i Europa Zachodnia kontra Chiny.

Masowe ataki ukierunkowane

W 2011 roku wyłoniły się nowe źródła szkodliwego oprogramowania i ukierunkowanych cyberataków. W nowym roku spodziewamy się znacznego wzrostu liczby nowych graczy oraz zagrożeń, jak również głośnych incydentów.

Do wzrostu liczby rejestrowanych ataków w pewnym stopniu przyczyni się znacznie skuteczniejszy proces wykrywania. Problemy związane z wykrywaniem i zwalczaniem ataków ukierunkowanych doprowadziły do wyłonienia się całkowicie oddzielnej dziedziny w branży bezpieczeństwa IT. Duże firmy, które padają ofiarą takich ataków, coraz częściej zwracają się o pomoc do małych prywatnych firm. Rosnąca konkurencja na rynku oferującym

takie usługi ochrony rzuci więcej światła na tego rodzaju incydenty. Na skutek wzrostu poziomu ochrony oraz liczby producentów oferujących pomoc w tym zakresie osoby atakujące będą zmuszone drastycznie zmienić swoje metody.

Obecnie wiele grup odpowiedzialnych za ataki ukierunkowane często nie zadaje sobie trudu stworzenia wyspecjalizowanego szkodliwego oprogramowania, wykorzystując zamiast tego cudze gotowe programy. Dobrym przykładem jest trojan Poison Ivy, który powstał w Szwecji, ale stał się ulubionym narzędziem chińskich hakerów. Jego przeciwieństwem jest trojan Duqu, który stanowi zapowiedź tego, co będzie, może zostać zmodyfikowany w zależności od określonych celów i wykorzystuje specjalizowane serwery kontroli.

Skuteczność tradycyjnych metod ataków – wykorzystywanie dokumentów w załącznikach do wiadomości e-mail, które zawierają szkodliwe programy atakujące poprzez luki w zabezpieczeniach – będzie stopniowo zmniejszać się. Ataki będą coraz częściej przeprowadzane z przeglądarek internetowych. Naturalnie, skuteczność takiego podejścia będzie zależała od liczby luk wykrytych w popularnym oprogramowaniu, takim jak przeglądarki, aplikacje biurowe czy systemy multimedialne.

Zwiększy się zakres atakowanych firm i obszarów gospodarki. Obecnie większość incydentów dotyka firmy oraz organizacje państwowe działające w przemyśle militarnym, w branży finansowej, hi-tech oraz badań naukowych. W 2012 roku ich celem staną się również firmy z sektora wydobycia zasobów naturalnych, energii, transportu, spożywczego i farmaceutycznego, jak również firmy świadczące usługi internetowe oraz z zakresu bezpieczeństwa IT. Znacznie zwiększy się również zasięg geograficzny ataków, który wykroczy poza Europę Zachodnią i Stany Zjednoczone i obejmie państwa w Europie Wschodniej, na Bliskim Wschodzie i w Południowo Wschodniej Azji.

Zagrożenia mobilne

Android

W 2012 r. niechciana popularność, jaką cieszy się platforma Android wśród twórców wirusów, jeszcze bardziej wzrośnie. Cyberprzestępcy atakujący platformy mobilne skoncentrują się głównie na tworzeniu szkodliwego oprogramowania dla Androida. Z powodu gwałtownego wzrostu liczby szkodliwych programów dla Androida w drugiej połowie 2011 r. system operacyjny Google'a uplasował się na pierwszym miejscu wśród mobilnych platform pod względem liczby zagrożeń i niewiele wskazuje na to, że twórcy wirusów pójdą w innym kierunku.

Spodziewamy się również wzrostu liczby ataków wykorzystujących luki w zabezpieczeniach. W 2012 roku cyberprzestępcy będą aktywnie stosować różne exploity w celu rozprzestrzeniania szkodliwego oprogramowania jak również szkodliwe programy zawierające exploity, które pozwalają na zwiększenie przywilejów i uzyskanie dostępu do systemu operacyjnego urządzenia. W 2011 r. praktycznie wszystkie ataki, w których wykorzystywane były luki w zabezpieczeniach, stanowiły próbę zwiększenia przywilejów w systemie operacyjnym. Z kolei w 2012 r. prawdopodobnie pojawią się pierwsze ataki, które będą wykorzystywały luki w celu zainfekowania samego systemu operacyjnego. Innymi słowy, będziemy świadkami pierwszych mobilnych ataków typu drive-by-download.

Zwiększy się liczba szkodliwych programów umieszczanych w sklepach z aplikacjami, szczególnie w Android Markecie. Mimo licznych szkodników wykrytych w jego oficjalnym sklepie Google nie zmienił znacząco zasad weryfikacji nowych aplikacji, w związku z czym twórcy wirusów prawdopodobnie nadal będą wykorzystywać go do rozprzestrzeniania swoich programów.

Istnieje duże prawdopodobieństwo pojawienia się pierwszego masowego robaka dla Androida, który będzie rozprzestrzeniał się za pośrednictwem wiadomości tekstowych i wysyłał odsyłacze prowadzące do sklepów z aplikacjami online, w których został umieszczony. Prawdopodobnie powstanie również pierwszy mobilny botnet (sieć zainfekowanych urządzeń) na tej platformie.

W 2011 r. aktywność kilku grup twórców szkodliwego oprogramowania specjalizujących się w aplikacjach mobilnych rozwinęła się w hurtową produkcję szkodliwego oprogramowania. Proces ten będzie widoczny również w 2012 r. To oznacza, że w przyszłym roku może już istnieć w pełni wykształcony przemysł mobilnego szkodliwego oprogramowania.

Inne mobilne platformy

- **Symbian.** Przez długi czas najpopularniejsza platforma zarówno wśród użytkowników jak i twórców wirusów. Obecnie traci pozycję na rynku mobilnych systemów operacyjnych oraz popularność wśród cyberprzestępców. Dlatego nie spodziewamy się znaczącej ilości szkodliwego oprogramowania dla tej platformy.

- **J2ME.** Nadal należy spodziewać się dość sporej ilości szkodliwych programów (a ściślej mówiąc, trojanów SMS) dla systemu Java 2 Micro Edition. Jednak ich liczba pozostanie na tym samym poziomie lub zmniejszy się.

- **Windows Mobile.** Platforma ta nigdy nie wzbudziła dużego zainteresowania wśród twórców wirusów. Rok 2011 nie był pod tym względem wyjątkiem. Nie będzie żadną niespodzianką, jeżeli liczbę szkodliwych programów dla tej platformy będzie można policzyć na placach jednej ręki.

- **Windows Phone 7.** Istnieje duże prawdopodobieństwo, że pojawi się pierwszy szkodnik typu proof-of-concept dla tej platformy.

- **iOS.** Od jego premiery w 2009 roku zostały wykryte dwa szkodliwe programy, których celem są przede wszystkim „złamane” urządzenia działające pod kontrolą tego systemu. W 2012 roku nie należy spodziewać się żadnych zmian w tym zakresie, chyba że Apple zmieni swoją politykę dystrybucji oprogramowania.

W 2012 roku wiele ataków ukierunkowanych będzie prawdopodobnie wykorzystywało szkodliwe oprogramowanie przeznaczone dla platform innych niż Android. Typowym przykładem jest atak przy użyciu programu ZitMo i SpitMo (ZeuS- oraz SpyEye-in-the-Mobile).

Mobilne szpiegostwo – kradzież danych z telefonów komórkowych oraz śledzenie osób przy użyciu ich telefonów oraz usług geolokalizacji – stanie się szeroko rozpowszechnione, wykraczając poza tradycyjne wykorzystywanie takich technologii przez organy ścigania i prywatne firmy detektywistyczne.

Ataki na bankowość online

W 2012 roku ataki na systemy bankowości online znajdą się w grupie do najbardziej rozpowszechnionych metod kradzieży pieniędzy należących do zwykłych użytkowników. Mimo stosowanych przez banki środków technicznych liczba przestępstw popełnianych w tym obszarze gwałtownie wzrasta na całym świecie.

W najbliższej przyszłości zwiększy się prawdopodobnie liczba przypadków nieautoryzowanego dostępu do systemów bankowości online w krajach azjatyckich. Przyczyni się do tego szybki rozwój takich usług w Azji Południowo-Wschodniej i Chinach oraz fakt, że liczni eksperci ds. cyberprzestępczości w tym regionie koncentrowali się do tej pory na innych typach ataków (w tym na atakach na fanów gier online). Oprócz atakowania użytkowników gier online azjatyccy cyberprzestępcy znani są z przeprowadzania ataków phishingowych na klientów europejskich i amerykańskich banków. Dzisiaj, gdy lokalne serwisy bankowe i płatności elektronicznych rozwijają się równolegle do wzrostu standardu życia w państwach azjatyckich, należy spodziewać się coraz większej liczby ataków na lokalne banki i użytkowników przy użyciu wyspecjalizowanych, lokalnych programów phishingowych i trojanów.

Celem takich ataków najprawdopodobniej będą użytkownicy urządzeń mobilnych oraz komputerów PC. Poza Azją Południowo-Wschodnią i Chinami mogą pojawić się ataki na mobilne serwisy płatności w krajach Afryki Wschodniej.

Prywatne życie użytkowników

Problem ochrony poufnych danych użytkowników staje się jednym z najgorętszych tematów bezpieczeństwa IT. W 2011 roku w Rosji miały miejsce wycieki danych, których ofiarą padli operatorzy sieci komórkowych oraz serwisy handlu elektronicznego. Oburzenie na świecie wywołało mobilne oprogramowanie CarrierIQ oraz informacje o przechowywaniu danych geolokacyjnych w iPhonie/iPadzie. Ponadto, do najgłośniejszych wydarzeń, jakie miały miejsce w zeszłym roku, należały kradzieże danych dotyczących dziesiątków milionów klientów różnych systemów w Korei Południowej oraz włamanie cyberprzestępców do Sony PlayStation Network. Mimo że incydenty te miały różne przyczyny i różniły się ilością oraz rodzajem skradzionych danych, wszystkie z nich miały ten sam cel.

Firmy na całym świecie próbują zebrać możliwie jak najwięcej informacji o swoich klientach. Niestety, nie idzie to w parze z odpowiednią ochroną przechowywanych informacji. Czynnikiem, który może sprzyjać utracie danych, jest nieustanny rozwój „technologii chmury": cyberprzestępcy mają teraz dodatkowy cel ataków, tj. centra danych, w których przechowywane są dane różnych firm. Wycieki danych z serwisów „w chmurze" mogą poważnie zaszkodzić reputacji tej technologii oraz koncepcji „przechowywania w chmurze", które w dużej mierze opierają się na zaufaniu użytkowników.

Jeżeli chodzi o systemy gromadzące dane o użytkownikach, takie jak CarrierIQ, jesteśmy przekonani, że w 2012 r. pojawi się więcej przypadków wykorzystywania takich systemów. Dostawcy usług telefonii komórkowej, producenci oprogramowania i usług sieciowych nie zamierzają odrzucić możliwości biznesowych, jakie daje posiadanie danych użytkowników.

Haktywizm

Haktywizm, czyli ataki hakerów w ramach protestu, przeżywa teraz swoiste odrodzenie i osiąga nowe poziomy. Mimo aresztowań znanych haktywistów w 2012 roku nadal będą miały miejsce liczne ataki na różne instytucje rządowe oraz biznesowe. Haktywizm będzie posiadał coraz więcej implikacji politycznych. Trend ten będzie jeszcze wyraźniejszy niż w 2011 r., gdy celem większości ataków przeprowadzanych na korporacje był tzw. „lulz", czyli forma naśmiewania się z kogoś.

Haktywizm może również być wykorzystywany jako przykrywka dla innych ataków, w celu odwrócenia od nich uwagi lub ustanowienia fałszywego tropu, umożliwiając „bezpieczne" włamanie się do danego obiektu. W 2011 roku wiele ataków haktywistów doprowadziło do wycieku poufnych danych, co bez wątpienia jest celem

klasycznych ataków ukierunkowanych, zarówno tych przeprowadzanych w ramach szpiegostwa handlowego jak i zabezpieczenia interesów narodowych. W takich przypadkach haktywiści (prawdopodobnie niechcący) oddali ogromną przysługę innym grupom, które mogą wykorzystać ich metody do kradzieży informacji podczas ataków innego typu.

Wnioski

Podsumowując, przewidujemy, że w następnym roku będą miały miejsce następujące wydarzenia oraz trendy w zakresie aktywności cyberprzestępczej:

- Cyberbroń w rodzaju robaka Stuxnet będzie „szyta na miarę", tj. tworzona tylko dla konkretnych celów. Cyberprzestępcy będą coraz częściej wykorzystywać prostsze narzędzia typu "kill switch", bomby logiczne itd. umożliwiające zniszczenie danych w określonym czasie.
- Zwiększy się liczba ataków ukierunkowanych. W związku ze spadkiem skuteczności obecnych metod infekcji cyberprzestępcy zaczną stosować nowe. Rozszerzy się również zakres atakowanych firm oraz obszarów działalności gospodarczej.
- W 2012 roku cyerprzestępcy będą pisali mobilne szkodliwe oprogramowanie, którego celem będzie głównie Android firmy Google. Przewidujemy wzrost liczby ataków wykorzystujących luki w zabezpieczeniach jak również pierwsze mobilne ataki drive-by (na przykład podczas przeglądania stron WWW).
- Odnotujemy coraz więcej przypadków umieszczania szkodliwego oprogramowania w oficjalnych sklepach z aplikacjami, głównie w Android Markecie. Rozpowszechni się szpiegostwo mobilne, obejmujące kradzież danych z telefonów komórkowych oraz śledzenie osób przy użyciu ich telefonów oraz usług geolokalizacji.
- W 2012 r. ataki na systemy bankowości online staną się jedną z najbardziej rozpowszechnionych metod kradzieży pieniędzy użytkowników. Najbardziej zagrożone będą kraje z Azji Południowo-Wschodniej, Chin i Afryki Wschodniej.
- Na całym świecie będą przeprowadzane liczne ataki na różne instytucje rządowe oraz firmy. Haktywizm może być wykorzystywany w celu ukrycia innych rodzajów ataków.