Jakich zagrożeń możemy się spodziewać w 2015 roku?

W dzisiejszych czasach kreatywność jest w cenie. Dotyczy to niestety także cyberprzestępców. Ofiarami nowych metod ataków w minionym roku zostali przede wszystkim użytkownicyurządzeń mobilnych, gracze korzystający z popularnych platform do gier multiplayer, a także klienci bankowości elektronicznej. Co nas zatem czeka w 2015 roku i jakie cele tym razem obiorą hakerzy? Specjaliści firmy antywirusowej Doctor Web przedstawiają prognozy zagrożeń.

Wirusy bankowe

W 2015 roku możemy spodziewać się dalszego rozwoju wirusów mających na celu wykradanie informacji o charakterze finansowym.Najbardziej narażeni na nie będą użytkownicy systemu Android. Powodem tego jest m.in. wzrost popularności urządzeń mobilnych, jako narzędzi do wykonywania operacji bankowych Coraz więcej instytucji finansowych wprowadza dedykowane aplikacje mobilne, które z kolei wzbudzają zainteresowanie przestępców.Coraz częściej dokonujemy też płatności na smartfonach, czy tabletach, z użyciem kart kredytowych.Dodatkowo nie pomaga fakt, że Android, jest platformą dużo mniej restrykcyjną w zakresie instalowania różnego rodzaju oprogramowania, niż np. system iOS, co czyni ją bardziej podatną na zagrożenia. Otwarty charakter Androida i łatwość dostępu do informacji o tym jak tworzyć programy na ten system, w tym programy złośliwe, to niezwykle istotny czynnik ryzyka dla jego użytkowników. Nowoodkryte luki w zabezpieczeniach potrafią być bardzo szybko i bezlitośnie wykorzystywane przez cyberprzestępców do kradzieży wrażliwych danych, w tym również tych finansowych.

W 2015 r. czeka nas też duża zmiana dotycząca płatności online. Komisji Nadzoru Finansowego, na skutek rekomendacji wydanej przez Europejski Bank Centralny, zobliguje banki do bardziej restrykcyjnego weryfikowania transakcji dokonywanych przez internet. Po wejściu zmian w życie to w Polsce nie będzie już można dokonywać płatności, jedynie z wykorzystaniem danych, które są widoczne na karcie. Oznacza to, że podanie numeru cvc z odwrotu karty, czy też daty jej ważności nie będzie wystarczające do zrealizowania transakcji.Zmiany te nie powinny być uciążliwe dla klientów, zwłaszcza w Polsce, gdzie karty kredytowe są stosunkowo mało popularne, a większość osób dokonuje płatności online innymi metodami. Z pewnością jednak wpłynie to pozytywnie na bezpieczeństwo przeprowadzania transakcji, gdyż dodatkowe zabezpieczenia zawsze tworzą dla oszustów dodatkową barierę.

Należy się liczyć również z tym, że w 2015 r. mogą pojawić się nowe Trojany bankowe dedykowane komputerom osobistym, szczególnie tym z systemem Windows. Przewidujemy jednak, że mechanizm ich działania będzie zapewne identyczny lub zbliżony do dotychczasowych zagrożeń tego typu, co z pewnością pomoże w opracowywaniu skutecznych metod walki z nimi.Zakładamy, że nowe wirusy będą więc przede wszystkim skupiać się na przechwytywaniu wprowadzanych danych, podmianie zawartości stron www, czy podmianie numerów telefonów służących do wysyłania potwierdzeń operacji.Jednym z najbardziej niebezpiecznych wirusów, które zostały odkryte przez laboratorium Doctor Web był Zeus p2p, działający w Polsce od 2011 roku.
Zagrożenia mobilne

Niezależnie od wirusów bankowych, które z pewnością będą wymierzone również w użytkowników tabletów, czy smarfonów, w 2015 r. należy spodziewać się większej ilości zagrożeń dla urządzeń mobilnych.W 2014 r. zaobserwowaliśmy powrót cyberprzestępców do pisania prostych wirusów, które tworzone są z pobudek ambicjonalnych, ideologicznych lub dla żartu. To jednak stosunkowo najmniej groźna odmiana złośliwego oprogramowania. Oprócz większej ilości tego typu programów, w dalszym ciągu należy się spodziewać poważniejszych wirusów, np.irytującychaplikacji wyświetlających niechciane reklamy oraz Trojanów blokujących urządzenia mobilne, które mogą zostać odblokowane dopiero po

zapłaceniu okupu.Ostatnia kategoria zagrożeń mobilnych, która najprawdopodobniej będzie nas nękać w 2015 r. to wirusy mające na celu nieautoryzowane wysyłanie kosztownych SMS-ów Premium, a także malware przeznaczone do instalowania innych złośliwych programów. Jako przykład można podać Android.Warmle.1.origin., który masowo wysyła wiadomości SMS, zawierające linki ze szkodliwą zawartością. Program został wykryty w listopadzie 2014 roku. Szacujemy, że w tym okresie zainfekował on ponad 14 tysięcy komputerów w 20 krajach na całym świecie.

Nowy cel ataków gracze

W świecie komputerów osobistych w 2014 roku pojawiło się kilka wirusów wymierzonych w nowe, nieatakowane dotychczas wirusami obszary.Przykładem są platformy onlinedla gier w trybie multiplayer. Jak dotąd sami tylko użytkownicy platformy Steam spotkali się z dwoma wirusami wykradającymi wartościoweelementy gier,posiadające realną wartość rynkową również poza wirtualnym światem.Oba Trojany (Trojana SteamBurglar.1 oraz Trojan.SteamLogger.1), które odkryli analitycy Doctor Web, nie muszą być ostatnimi, gdyż rynek gier wideo jest coraz atrakcyjniejszym celem dla cyberprzestępców.Kolejną po Steam-ie zagrożoną platformą może być jej konkurent rynkowy - platformaOrigin.
Nie tylko Microsoft Windows

Podobnie jak miało to miejsce w minionych 12 miesiącach, tak również w 2015 użytkowników komputerów nadal będą atakować Trojany w formie wtyczek do przeglądarek www, odpowiedzialne za wyświetlanie niechcianych reklam i za klikanie w nie bez wiedzy i zgody użytkownika. Z całą pewnością przestępcy nie zrezygnują też z prób atakowania alternatywnych systemów operacyjnych dla PC i serwerów (Linux i Mac OS X), tym bardziej, że procent maszyn z zainstalowanym oprogramowaniem antywirusowym jest w ich przypadku znacznie niższy, niż w świecie różnych odmian Microsoft Windows.Ponadto instalacje serwerowe, szczególnie z systemami Linux/Unix, realizują często bardzo ważne zadania i usługi, będąc tym samym atrakcyjnym celem dla cyberprzestępców. Jedynie w przypadku systemów iOS i Windows Phone można zaryzykować stwierdzenie, że utrzymają one swój status niezdobytych , a przynajmniej niezwykle trudno dostępnych, dzięki konsekwentnie realizowanej przez ich autorów restrykcyjnej politycebezpieczeństwa. Pamiętajmy jednak, że nigdy nie możemy być pewni, czy przestępcy nie znajdą sposobu, aby kiedyś zaistnieć w świecie mobilnych jabłek i okienek .

Mniej botnetów w 2015?

Patrząc na dotychczasowe tendencje możemy spodziewać się spadku znaczenia i liczebności botnetów. Trend ten odwrócić może jedynie jakieś nowe, wyjątkowo złośliwe lub wyjątkowo dochodowe zagrożenie tego typu. Największym jak dotąd botnetem w historii, odkrytym przez analityków Doctor Web był wirus z rodziny Anroid.Sms.Send. Głównym źródłem infekcji były w tym przypadku strony będące własnością cyberprzestępców oraz witryny zaatakowane i kontrolowane przez nich po to, aby rozpowszechniać dalej szkodliwe oprogramowanie. Niebezpiecznym botnetem, odkrytym w 2014 roku był Win32.Rmnet.12złożony z komputerów z systemem Windows. W marcu 2014 roku średnia liczba botów w pierwszej podsieci, monitorowanej przez analityków bezpieczeństwa Doctor Web, osiągnęła liczbę 244 430. Pod koniec marca ilość komputerów zainfekowanych tym wirusem uległa zmniejszeniu.
Wyścig trwa

Ze wszystkich niebezpieczeństw, jakie czyhać będą na nas w 2015 r. najbardziej niepokojące wydają się być nowe wirusy o charakterze finansowym, które wykorzystują nie tyle naiwność, co zwyczajny brak świadomości zagrożeń z ich strony u użytkowników bankowości elektronicznej, dotoczy to również banków w Polsce. Za ogólnym rozwojem technologii i rosnącą liczbą nowych użytecznych metod wykorzystywania internetu idzie również rozwój cyberzagrożeń. Wyścig pomiędzy przestępcami, a specjalistami od cyfrowego bezpieczeństwa trwa od dawna i nie zanosi się by wyhamował w 2015 r.

Autor: Piotr Tyborowski, specjalista ds. bezpieczeństwa z firmy Doctor Web.