**Koniec odporności: krótka opowieść o bezpieczeństwie systemów firmy Apple**

**Przez wiele lat firma Apple, wraz ze swoimi najwierniejszymi fanami, dumnie utrzymywała, że dysponuje platformą wolną od szkodliwych programów. Czasy te jednak bezpowrotnie minęły. Wraz z tym, jak udział maszyn Apple’a w rynku osiągał coraz wyższy poziom, cyberprzestępcy zaczęli postrzegać systemy z nadgryzionym jabłkiem jako potencjalne źródło zysku. Eksperci z Kaspersky Lab podsumowali najnowsze incydenty związane z bezpieczeństwem systemów firmy Apple.**

Żyjemy w czasach, w których żadna platforma, łącznie z Apple, nie może być traktowana jako odporna na zagrożenia. Systemy Apple’a są w rzeczywistości atakowane z kilku kierunków. Badacze i cyberprzestępcy znajdują coraz to nowe luki w zabezpieczeniach, a ci drudzy dodatkowo tworzą metody, które pozwalają je wykorzystać do przeprowadzania ataków. Pod ostrzałem są urządzenia mobilne, tradycyjne komputery, a nawet usługi działające w chmurze.

Całkiem niedawno badacze z jednego z uniwersytetów w Niemczech [rozszyfrowali metodę](http://www.kaspersky.pl/about.html?s=newsspecial&amp;amp;newsid=2000) wykorzystywaną przez system iOS do tworzenia domyślnych haseł dla mobilnych hotspotów Wi-Fi, które mogą aktywować niemal wszyscy posiadacze iPhone’ów i iPadów (w zależności od użytkowanego modelu). Okazało się, że hasła te składają się zawsze z jednego słowa i czterech cyfr. Po odkryciu serii słabości w sposobie generowania słów naukowcy byli w stanie za każdym razem łamać domyślne hasło w czasie krótszym niż jedna minuta.

Tuż po pojawieniu się wersji beta systemu iOS 7 pewien Brazylijczyk zdołał bez większych problemów obejść blokadę ekranu. Fakt, mówimy o wersji beta, która z założenia może posiadać wiele rozmaitych błędów, jednak w tym przypadku system został pobrany przez wielu użytkowników i niekoniecznie byli to programiści czy eksperci.

Odtwarzacz muzyczny Apple’a – iTunes – i jego popularny sklep z aplikacjami App Store ucierpiały w wyniku ataków phishingowych. Doszło nawet do przejęcia kont użytkowników. Incydenty te nie były specjalnie spektakularne aż do niedawna, gdy eksperci z Kaspersky Lab [odnotowali dramatyczny wzrost liczby ataków phishingowych](http://securelist.pl/blog/7232,jablko_niezgody.html), mających na celu przejęcie identyfikatorów Apple ID i danych finansowych użytkowników. Warto wiedzieć, że Apple ID jest swego rodzaju kluczem dającym dostęp do wszystkich usług i kont w serwisach Apple.

Z myślą o zwiększeniu bezpieczeństwa Apple wprowadził w tym roku dwuetapową weryfikację, co oczywiście jest dobrym krokiem. Niestety, firma stworzyła także system resetowania haseł, który – w wyniku błędów – można było wykorzystać do przejęcia kont innych użytkowników. W efekcie firma Apple była zmuszona do zamknięcia tej usługi na pewien czas, by usunąć krytyczne problemy.

Nowe szkodliwe programy dla Maków pojawiają się szybciej niż kiedykolwiek wcześniej. Niedawno pojawiło się oszustwo imitujące wiadomość od FBI, w której cyberprzestępcy próbowali szantażować użytkowników systemu OS X. Praktycznie co miesiąc pojawia się informacja o atakach na korzystających z Maków aktywistów ujgurskich i tybetańskich. Często dowiadujemy się także o nowych backdoorach dla systemu OS X, które pozwalają cyberprzestępcom przejmować kontrolę nad zainfekowanymi Makami, a całkiem niedawno doszło do ataku na stronę Apple’a przeznaczoną dla programistów.

Poza tymi wszystkimi incydentami istnieją także [ataki uniwersalne](http://www.kaspersky.pl/about.html?s=newsspecial&amp;amp;newsid=1986), które potrafią automatycznie wykryć platformę, na jakiej są uruchomione, i zastosować odpowiedni zestaw narzędzi do przeprowadzenia infekcji.

*„Ostatecznie, patrząc na to wszystko z boku, nie ma znaczenia, z jakiej platformy korzysta użytkownik. Jeżeli cyberprzestępcy zwietrzą w niej pieniądze lub cenne dane, które można ukraść, dany system prędzej czy później stanie się dla nich intratnym celem”* – powiedział Maciej Ziarek, ekspert ds. bezpieczeństwa, Kaspersky Lab Polska. *„Na szczęście jednak użytkownicy nie są bezbronni i mogą zadbać o bezpieczeństwo, zachowując czujność, instalując dobry program antywirusowy i regularnie uaktualniając wszystkie aplikacje oraz system operacyjny”.*

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.