**Coraz więcej szkodliwych programów atakuje konta bankowe online**

**Kaspersky Lab informuje o wzroście ilości szkodliwego oprogramowania potrafiącego kraść pieniądze użytkowników kont bankowych online. W badanym okresie, od 19 kwietnia do 19 maja 2014 r., rozwiązania firmy Kaspersky Lab zablokowały 341 216 prób uruchomienia takich niebezpiecznych aplikacji – o 36,6% więcej w stosunku do poprzedniego miesiąca.**

Ponad jedna trzecia łącznej liczby użytkowników zaatakowanych przez szkodliwe oprogramowanie bankowe znajdowała się w Brazylii, Rosji i we Włoszech. Nagły wzrost aktywności szkodliwego oprogramowania bankowego najprawdopodobniej ma związek z początkiem sezonu wakacyjnego, gdy klienci aktywnie wykorzystują swoje dane płatnicze do dokonywania różnego rodzaju zakupów online.

**Jakie dane najchętniej kradną cyberprzestępcy?**

Zwykle cyberprzestępcy próbują kraść szczegóły dotyczące kart bankowych użytkowników przy użyciu wyspecjalizowanych programów trojańskich. Od połowy kwietnia do połowy maja ZeuS ([Trojan-Spy.Win32.Zbot](http://www.kaspersky.pl/about.html?s=news_warnings&amp;amp;cat=4&amp;amp;newsid=2231)) po raz kolejny był najbardziej rozpowszechnionym trojanem bankowym. Według badań Kaspersky Lab, program ten został wykorzystany w 198 200 próbach infekcji klientów bankowości online. Około 82 300 osób atakowano przy użyciu szkodliwych programów rozprzestrzenianych głównie za pośrednictwem spamowych wiadomości e-mail z tematem „Opłaty za bankowość internetową” - Trojan-Banker.Win32.ChePro i Trojan-Banker.Win32.Lohmys.

Inną metodą kradzieży danych bankowych są ataki phishingowe. W badanym okresie rozwiązania firmy Kaspersky Lab zablokowały 21,5 miliona takich ataków, a celem prawie 10% z nich (około 2 miliony) były szczegóły dotyczące kart bankowych.

**Luka Heartbleed dalej zbiera swoje żniwo**

W badanym okresie można było zauważyć konsekwencje zdarzenia, które poważnie zagroziło bezpieczeństwu systemów płatności online. Mowa tu o luce [Heartbleed](http://plblog.kaspersky.com/2014/04/10/luka-heartbleed-moze-obejsc-twoje-zabezpieczenia-na-tysiacach-stron/), która została wykryta wcześniej w popularnej bibliotece szyfrowania OpenSSL. Dziura ta pozwala osobom atakującym uzyskać nieautoryzowany dostęp do pamięci podatnego na ataki urządzenia, takiego jak smartfon, komputer PC czy serwer. Luka nie pozostawia żadnego śladu i nadal nie wiadomo, jakie dane i w jakich ilościach zostały skradzione. Dobrą informacją jest to, że większość firm przeprowadzających transakcje online przy użyciu dziurawej wersji OpenSSL zalecało swoim klientom, aby zmienili hasło do konta i zwracali uwagę na wszelką nietypową aktywność.

„Pojawienie się luki Heartbleed zapoczątkowało serię wycieków różnego rodzaju danych w różnych branżach biznesowych. Powodem było to, że luka znajdowała się w kryptograficznej bibliotece OpenSSL, która jest wykorzystywana w różnych narzędziach, łącznie z oprogramowaniem bankowym” – skomentował **Siergiej Golowanow**, główny badacz ds. bezpieczeństwa w Kaspersky Lab. „Brak oficjalnej aktualizacji biblioteki przez kilka godzin po wykryciu luki oraz opieszałość działów bezpieczeństwa IT w instytucjach finansowych w instalowaniu aktualizacji prowadził w niektórych przypadkach do wycieku danych dotyczących transakcji bankowych. W związku z tym w następnych miesiącach spodziewamy się wzrostu liczby oszukańczych transakcji”.

Miesięczne raporty dotyczące zagrożeń online w sektorze bankowym to tylko jedna z usług analiz oferowanych przez Kaspersky Lab w ramach platformy [Kaspersky Fraud Prevention](http://www.kaspersky.pl/about.html?s=news_products&amp;amp;cat=5&amp;amp;newsid=2199). Rozwiązanie to zapewnia wielopoziomową ochronę płatności elektronicznych i zapobiega oszustwom finansowym online. Kaspersky Fraud Prevention integruje komponenty serwerowe zainstalowane na sprzęcie instytucji finansowych, aplikacje klienckie dla punktów końcowych oraz wyspecjalizowane usługi informatyczne.

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>.