**Nowa międzynarodowa wersja mobilnego trojana finansowego**

**8 czerwca eksperci z Kaspersky Lab wykryli nową wersję trojana mobilnego o nazwie Svpeng, która działa obecnie w Stanach Zjednoczonych oraz Wielkiej Brytanii i łączy w sobie funkcjonalność szkodnika finansowego z możliwościami oprogramowania wyłudzającego okup (tzw. ransomware).**

Twórcy tego zagrożenia po raz pierwszy zastosowali podejście międzynarodowe – dotychczas Svpeng kradł pieniądze wyłącznie w Rosji. Szkodnik atakuje urządzenia mobilne z systemem Android.

Na chwilę obecną nowa wersja trojana Svpeng nie kradnie danych uwierzytelniających, jest jednak kwestią czasu, zanim tak się stanie, ponieważ szkodnik stanowi modyfikację znanego trojana, który działa w Rosji i jest wykorzystywany głównie do kradzieży pieniędzy. Ponadto, kod trojana zawiera pewne odniesienia do metody „Cryptor”, która nie została jeszcze zastosowana, dlatego istnieje prawdopodobieństwo, że wkrótce będzie wykorzystana do szyfrowania plików. W takiej sytuacji, Svpeng zostanie drugim najbardziej znanym mobilnym szkodliwym programem z taką funkcjonalnością. Pierwszy, Pletor, pojawił się na wolności w maju 2014 r.

Svpeng sprawdza telefon użytkownika w poszukiwaniu listy określonych aplikacji finansowych – prawdopodobnie w celu wykorzystania tych danych w przyszłości, gdy rozpocznie kradzież loginów/haseł do serwisów bankowości online, tak jak robi to już w przypadku kont banków rosyjskich. Anglojęzyczny Svpeng sprawdza obecność następujących aplikacji na urządzeniu ofiary:

- USAA Mobile,

- Citi Mobile,

- Amex Mobile,

- Wells Fargo Mobile,

- Bank of America Mobile Banking,

- TD App,

- Chase Mobile,

- BB&T Mobile Banking,

- Regions Mobile.

Następnie szkodnik blokuje ekran urządzenia mobilnego imitacją powiadomienia o karze FBI oraz żąda 200 dolarów zapłaty za przywrócenie dostępu.

Obecnie celem ponad 91% ataków są anglojęzyczni użytkownicy zlokalizowani w Stanach Zjednoczonych i Wielkiej Brytanii. Pozostałe 9% stanowią ataki na Indie, Niemcy i Szwajcarię. Niedługo zasięg trojana może objąć również inne państwa i języki.

„Odparcie ataku anglojęzycznej wersji trojana Svpeng jest niemożliwe, jeżeli urządzenie mobilne nie posiada rozwiązania bezpieczeństwa – szkodnik całkowicie zablokuje urządzenie, a nie oddzielne pliki jak miało to miejsce w przypadku jednego z poprzednich zagrożeń tego typu - [Cryptolockera](http://plblog.kaspersky.com/2014/05/29/cryptolocker-dla-androida/). Szansa na odblokowanie urządzenia istnieje wyłącznie wtedy, gdy przed infekcją użytkownik uzyskał prawa administratora w procesie tzw. [rootowania](http://plblog.kaspersky.com/2014/06/11/rootowanie-i-jailbreaking-na-czym-polegaja-i-jaki-maja-wplyw-na-bezpieczenstwo/). W takim wypadku można je odblokować bez usuwania danych. Inną opcją jest usunięcie trojana – jeżeli telefon nie został zrootowany, należy uruchomić go w trybie bezpiecznym i skasować wszystkie dane zapisane w samym urządzeniu – infekcja zostanie usunięta, a informacje zapisane na karcie SIM oraz SD pozostaną nietknięte” – tłumaczy **Roman Unuchek**, starszy analityk szkodliwego oprogramowania, Kaspersky Lab.

Produkty firmy Kaspersky Lab wykrywają szkodliwy program Svpeng jako Trojan-Banker.AndroidOS.Svpeng.a.

Rozwiązania bezpieczeństwa firmy Kaspersky Lab przeznaczone dla użytkowników indywidualnych i korporacyjnych zawierają szereg technologii zapobiegających różnym rodzajom ataków szkodliwego oprogramowania w tym takich, których celem jest kradzież danych finansowych lub szyfrowanie ważnych plików w celu wyłudzania okupu.

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>.