**Niepokojący wzrost liczby zagrożeń dla danych w III kwartale 2013 r.**

**Eksperci z Kaspersky Lab przygotowali najnowszy przegląd krajobrazu cyberzagrożeń. Trzeci kwartał 2013 r. stanowił punkt zwrotny dla twórców szkodliwego oprogramowania specjalizujących się w platformach mobilnych.**

W czerwcu eksperci wykryli nowego trojana o nazwie Svpeng, który potrafi uzyskiwać dostęp do konta bankowego ofiary bezpośrednio z jej smartfona. Jest to znacznie prostsza droga niż konwencjonalna ścieżka smartfon plus komputer wykorzystywana zwykle przez tego typu szkodliwe oprogramowanie.

We wrześniu wykryto pierwsze przypadki botnetów osób trzecich wykorzystywanych do rozprzestrzeniania trojanów. To znacznie rozszerza zakres infekcji i stanowiło klucz do rozprzestrzeniania Obada - najbardziej wyrafinowanego trojana dla Androida spośród zidentyfikowanych do tej pory.

W przeciwieństwie do innych szkodliwych programów tego typu (ZitMo, SitMo) Svpeng pozwala cyberprzestępcom kraść pieniądze po zainfekowaniu zaledwie jednego urządzenia – smartfona ofiary. Szkodnik sprawdza stan konta za pośrednictwem serwisu bankowości mobilnej, otrzymuje odpowiedź oferującą doładowanie konta mobilnego ofiary i przelewa pieniądze z konta bankowego użytkownika na mobilne konto cyberprzestępcy. Atakujący mogą przesłać środki do swoich portfeli cyfrowych i zamienić je na gotówkę. Trojan Svpeng może narazić swoje ofiary na straty w wysokości tysięcy dolarów.

Według Kaspersky Lab celem 99,9% wszystkich ataków na platformy mobilne jest Android. Wiktor Czebyszew, analityk wirusów w Kaspersky Lab, powiedział: *„Większość szkodliwego oprogramowania dla Androida jest tworzona w celu kradzieży pieniędzy lub, dodatkowo, danych osobistych. Szybko adoptowane są wszystkie znane mechanizmy dystrybucji i zacierania śladów stosowane w odniesieniu do komputerów PC. Dzisiaj cyberprzestępcy robią wszystko, co tylko się da, aby ukraść możliwie jak najwięcej. Twórcy wirusów prawdopodobnie nadal będą zwiększać liczbę botnetów, infekując coraz więcej użytkowników Androida”.*

Podczas gdy cyberprzestępcy, których celem są platformy mobilne, rozwijają coraz bardziej wyrafinowane metody, ataki sieciowe nadal bazują na liczbie incydentów. W III kwartale 2013 r. produkty firmy Kaspersky Lab wykryły łącznie 500 284 715 ataków. W dziesięciu państwach znajdowało się 81,5% zasobów sieciowych wykorzystywanych do dystrybucji szkodliwego oprogramowania, przy czym na prowadzeniu znalazły się Stany Zjednoczone, Rosja i Niemcy.

**Ataki ukierunkowane/APT w III kwartale 2013 r.**

We wrześniu Kaspersky Lab wykrył niewielką, ale aktywną grupę APT o nazwie [Icefog](http://www.kaspersky.pl/about.html?s=news_press&amp;amp;cat=1&amp;amp;newsid=2103), która koncentruje się na celach w Korei Południowej oraz Japonii i atakuje łańcuchy dostaw zachodnich firm. Charakter ataków grupy Icefog wskazuje na wyłanianie się nowego trendu: działalności małych gangów, które z chirurgiczną precyzją polują na konkretne informacje.

W III kwartale specjaliści ds. bezpieczeństwa z Kaspersky Lab analizowali również aktywną kampanię cyberszpiegowską, której głównym celem były grupy ekspertów w Korei Południowej. Kampania ta, znana pod nazwą [Kimsuky](http://www.kaspersky.pl/about.html?s=news_warnings&amp;amp;cat=4&amp;amp;newsid=2085), ma ograniczony zasięg i jest wysoce ukierunkowana. Analizy techniczne wykazały, że osoby atakujące były zainteresowane głównie organizacjami znajdującymi się w Korei Południowej oraz dwiema grupami w Chinach. Znalezione przez ekspertów z Kaspersky Lab tropy sugerują, że osoby atakujące pochodzą z Korei Północnej.

Więcej informacji na temat rozwoju sytuacji związanej ze szkodliwym oprogramowaniem w III kwartale 2013 r. znajduje się w pełnym raporcie, opublikowanym w serwisie [SecureList.pl](http://securelist.pl) prowadzonym przez Kaspersky Lab.

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>.