**Trojan Stealer - jedno z najbardziej aktywnych zagrożeń dla Androida**

**Krajobraz zagrożeń mobilnych ewoluuje w błyskawicznym tempie, a liczba nowych szkodliwych programów nieustannie rośnie. Niektóre z nich są jednak rozpowszechnione w szczególnym stopniu i odpowiadają za większość prób infekowania użytkowników smartfonów oraz tabletów.**

Jest tak w przypadku SMS-owego trojana Stealer atakującego urządzenia z Androidem, któremu przyjrzeli się bliżej eksperci z Kaspersky Lab.

Szkodliwy program Trojan-SMS.AndroidOS.Stealer.a stał się w ciągu roku liderem w liczbie prób infekowania użytkowników i w dalszym ciągu okupuje czołowe miejsca w zestawieniach najbardziej aktywnych zagrożeń mobilnych. W pierwszym kwartale 2014 r. odpowiadał on za niemal 25% wszystkich ataków mobilnych.

Cyberprzestępcy odpowiedzialni za trojana Stealer są najbardziej aktywni w Rosji, jednak eksperci z Kaspersky Lab wykryli wiele ataków tego szkodnika niemal na całym świecie.

**Możliwości trojana**

Popularność i szerokie rozprzestrzenienie Stealera wynika w dużej mierze z jego możliwości, a konkretniej z wyposażenia go przez twórców w łatwy w modyfikowaniu plik konfiguracyjny. Szkodnik wykrywa w jakim regionie jest uruchomiony i odpowiednio modyfikuje treści wysyłanych szkodliwych SMS-ów oraz numery potencjalnych ofiar. Stealer rozprzestrzenia się pod przykrywką legalnej aplikacji i po instalacji działa w tle.

Trojan jest zarządzany przez dwa niezależne serwery kontrolowane przez cyberprzestępców - pierwszy odpowiada za przydzielanie zadań, a drugi odbiera wszystkie rezultaty działania szkodnika. Wszystkie dane przesyłane przez trojana są szyfrowane. Zaszyfrowany jest także plik konfiguracyjny wykorzystywany przez cyberprzestępców do modyfikowania funkcjonalności Stealera. Bazowy zestaw funkcji obejmuje m. in. następujące działania:

zmień serwer kontroli,

usuń wiadomości przychodzące,

uaktualnij się,

wyślij informacje o zainfekowanym telefonie,

wyślij listę zainfekowanych aplikacji,

usuń wybraną aplikację,

otwórz wybraną stronę WWW,

pobierz położenie geograficzne urządzenia,

filtruj przychodzące SMS-y,

przechwytuj wszystkie wiadomości,

wyślij SMS-a na numer zdefiniowany w pliku konfiguracyjnym,

zainstaluj wskazaną aplikację,

ukrywaj komunikaty systemowe.

Zmieniając zawartość pliku konfiguracyjnego cyberprzestępcy mogą modyfikować funkcjonalność Stealera. Plik konfiguracyjny jest dołączany do każdej kopii trojana, w wyniku czego jego szkodliwa aktywność może być kontynuowana nawet, gdy zainfekowany smartfon nie ma aktywnego połączenia z internetem.

Eksperci z Kaspersky Lab spodziewają się dalszego wzrostu liczby prób infekcji wykorzystujących szkodliwy program Trojan-SMS.AndroidOS.Stealer.a. Aby jeszcze bardziej zwiększyć zasięg szkodnika, cyberprzestępcy najprawdopodobniej będą sukcesywnie zmniejszać jego rozmiar, zachowując jednocześnie pełną funkcjonalność.

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>.