Śledzić wszystkich

20 listopada 2016

Amerykańska firma Kryptowire, specjalizująca się w środkach analizy bezpieczeństwa systemów mobilnych i aplikacji multimedialnych, poinformowała o znalezieniu w oprogramowaniu setek tysięcy smartfonów komponentu, który kopiuje korespondencję użytkowników na chińskie serwery.

Najczęściej dane o użytkownikach są zbierane za pomocą nieudokumentowanych funkcji różnych aplikacji mobilnych. Czasami odbywa się to w celu identyfikacji nawyków właścicieli oraz dalszej poprawy jakości świadczonych usług serwisu. W innych przypadkach na podstawie zebranych informacji użytkownikowi pokazuje się reklama tematyczna lub składane są inne propozycje handlowe. Ale nie tylko.

Aby ocenić skalę tego nadzoru wystarczy odnieść się do zeszłorocznego raportu firmy Eurecam. Zawiera on rezultaty analizy dwóch tysięcy darmowych aplikacji z Google Play, w 30% których odnotowano próbę wymiany danych z 250 tysiącami adresów internetowych, umieszczonych na dwóch tysiącach domen drugiego poziomu. Większość z tych kontaktów dotyczyła wbudowanej reklamy, ale druga część okazała się być powiązana z przekazywaniem danych użytkownika i złośliwego oprogramowania.

Na przykład popularna w Europie aplikacja Eurosport Player, która została pobrana przez kilka milionów użytkowników, nawiązywała połączenie z 810 różnymi witrynami trekkingowymi.

Według wspomnianej na początku Kryptowire udało jej się znaleźć w oprogramowaniu kilku smartfonów amerykańskiej firmy BLU Products komponent, który zbiera całą korespondencję użytkownika, dane z książki adresowej, historię połączeń i lokalizację użytkownika i co 72 godziny wysyła wszystko na chińskie serwery.

To szpiegowskie oprogramowanie zostało opracowane przez firmę Shanghai Adups Technology Company, która jest dużym dostawcą usług wymiany oprogramowania „przez chmurę” dla dużej liczby firm i operatorów na całym świecie. Obecnie obsługuje ona 700 milionów abonentów w 200 krajach.

Firma BLU Products niezwłocznie złożyła swoje pretensje do Adups Technology. W odpowiedzi Chińczycy oświadczyli, że moduły śledzenia z oprogramowania dla telefonów BLU zostały już usunięte, a dane zgromadzone na serwerach całkowicie usunięte.

Skandal z Adups Technologii może wydawać się mało znaczący, gdyby wśród jej kluczowych partnerów nie było dwóch największych chińskich firm Huawei i ZTE.

Obie te firmy w pewnym momencie zostały wyparte z amerykańskiego rynku ze względu na podejrzenie o obecność w ich komunikacyjnej instalacji szpiegowskich modułów. A za ich plecami amerykańskie służby bezpieczeństwa stale widziały chiński rząd.

Początkowo taka reakcja była spowodowana wojskową przeszłością jednego z założycieli Huawei Rena Zhengfeia, byłego kadrowego oficera armii Chin. A potem pojawiły się inne podejrzenia. Dlatego Waszyngton zaczął przeszkadzać w pracy firmy we wszystkich głównych obszarach związanych z dostawami sprzętu, oskarżając ją o współpracę z chińskimi służbami specjalnymi.

„Zupełnie mnie to nie zaskakuje, biorąc pod uwagę ostatnie skandale wokół firmy Huawei, której pozbawiono dostępu do amerykańskiego rynku w 2014 roku ze względu na fakt, że firma została posądzona o zainstalowanie pluskiew w sprzęcie” – komentuje sytuację Andriej Sołdatow, dziennikarz i redaktor naczelny witryny agentura.ru.

W swoich komentarzach Adups Technology w pełni zaprzecza związkom z rządem Chin, a jej amerykański adwokat twierdzi, że wszystko, co się stało – to niefortunny błąd prywatnej firmy.

Poinformowano również, że dane miały być gromadzone na wniosek jednego z chińskich producentów i tylko na jego urządzeniach.

Tymczasem Kryptowire uważa, że podobne szpiegowskie moduły mogą być obecne także w innych smartfonach. Najwięcej obaw wyrażają w związku z niedrogimi modelami operatorskimi, które są dość popularne w Stanach Zjednoczonych. Z reguły ich bezpieczeństwu poświęca się nie tak wiele uwagi zarówno ze strony użytkowników, jak i ekspertów.

Źródło: pl.SputnikNews.com