**HummingBad zagraża nawet 10 mln urządzeń!**

**Przez pięć miesięcy, badacze zagrożeń mobilnych z firmy Check Point posiadali niespotykaną wcześniej możliwość dostępu do wewnętrznej grupy roboczej Yingmob, czyli chińskich cyberprzestępców stojących za kampanią malware zwaną HummingBad.**

HummingBad jest złośliwym oprogramowaniem, które jak odkrył Check Point instaluje złośliwe aplikacje, generując przy tym wysokie przychody z równie złośliwych dla użytkownika reklam.

Co ciekawe, wg ekspertów bezpieczeństwa, Yingmob działa obok legalnie funkcjonującej w Chinach agencji analiz reklam z którą dzieli swoje zasoby i technologie. Według doniesień, skład liczący 25 pracowników jest bardzo dobrze zorganizowany i składa się z czterech niezależnych grup odpowiedzialnych za rozwój szkodliwych komponentów HummingBad.

Wcześniej część firm badawczych łączyła Yingmob jedynie z Yispecte, oprogramowaniem malware działającym pod systemem iOS. Jednak najnowsze analizy firmy Check Point mogą potwierdzać, że ta sama grupa stoi najprawdopodobniej za HummingBad. Dotychczasowe śledztwo wykazało, że:

l Yispecter używa certyfikatów dla przedsiębiorstw Yingmob by zainstalować się na urządzeniach;

l HummingBad i Yispecter dzielą te same adresy serwerów C&C;

l repozytoria HummingBad zawierają dokumentację QVOD, odtwarzacz filmów porno działający w urządzeniach z systemem iOS, który kierowanego przez Yispecter;

l Obie aplikacje instalują złośliwe aplikacje w celu generowania zysków.

Yingmob używa HummingBad do kontroli 85 mln urządzeń na całym świecie, które generują miesięcznie 300 tys. dolarów pochodzących z nielegalnych reklam! Ten stały strumień gotówki, w połączeniu ze skupioną strukturą organizacyjną, dowodzi, że cyberprzestępcy mogą łatwo stać się finansowo całkowicie samowystarczalni.

Ośmielony swoją niezależnością, Yingmob i inne podobne grupy, mogą szlifować swoje umiejętności w prowadzeniu kampanii malware, obierając zupełnie nowe kierunki, twierdzą badacze Check Pointa. Przykładowo, grupy mogą łączyć urządzenia w celach stworzenia potężnego botnetu, tworzyć bazy danych urządzeń w celu prowadzenia wysoce ukierunkowanych ataków czy tworzyć nowe źródła zysków, sprzedając dostęp do kontrolowanych urządzeń.

Bez możliwości wykrywania i zatrzymania podejrzanych zachowań, miliony urządzeń z Androidem wraz z danymi pozostają narażone na coraz bardziej zawansowane ataki.