Kaspersky Lab: cybergang Roaming Mantis atakuje smartfony

ID artykułu: 54032 / 2264

URL: http://www.publikuj.org/54032

Badacze z Kaspersky Lab wykryli nowe szkodliwe oprogramowanie dla systemu Android rozpowszechniane z użyciem techniki przechwytywania ustawień DNS, atakujące głównie w Azji.

Kampania cyberprzestępcza, nazwana Roaming Mantis, pozostaje aktywna i ma na celu kradzież informacji użytkowników, łącznie z danymi logowania, a także pozwala atakującym na przejęcie kontroli nad zainfekowanymi urządzeniami mobilnymi. W okresie luty-kwiecień 2018 r. badacze wykryli to szkodliwe oprogramowanie głównie w Korei Południowej, Bangladeszu oraz Japonii, jednak z dużym prawdopodobieństwem istnieją także ofiary zlokalizowane w innych częściach świata. Zdaniem ekspertów z Kaspersky Lab cyberprzestępcy stojący za operacją są motywowani chęcią zysku.

Z badań Kaspersky Lab wynika, że atakujący stojący za omawianymi atakami szukają routerów podatnych na ataki i dystrybuują szkodliwe oprogramowanie z użyciem prostego triku polegającego na przechwyceniu ustawień DNS w tych urządzeniach sieciowych. Sama metoda wykorzystywana do atakowania routerów pozostaje nieznana. Gdy ustawienia DNS zostaną zmodyfikowane, użytkownik, który chce otworzyć dowolną stronę WWW, widzi na ekranie witrynę o prawidłowym adresie, jednak treść jest podstawiana z serwera kontrolowanego przez cyberprzestępców. Zawiera ona komunikat informujący użytkownika, że w celu zwiększenia komfortu przeglądana internetu należy zainstalować nową wersję przeglądarki. Kliknięcie wyświetlanego odnośnika inicjuje instalację konia trojańskiego, który umożliwia atakującym przejęcie kontroli nad zainfekowanym urządzeniem z Androidem.

Szkodliwe oprogramowanie Roaming Mantis sprawdza, czy zainfekowane urządzenie zostało zrootowane (proces dający dostęp do uprawnień administratora w systemie Android) i przechwytuje informacje o wszelkiej aktywności użytkownika związanej z przeglądaniem zasobów internetu. Szkodnik potrafi gromadzić szereg informacji, łącznie z danymi uwierzytelniającymi. Badacze odkryli, że fragmenty kodu szkodliwego programu odnoszą się do popularnych w Korei Południowej aplikacji bankowych i gier.

Wstępna analiza Kaspersky Lab wykazała około 150 ofiar, jednak dalsze badanie ujawniło, że każdego dnia kilka tysięcy zainfekowanych urządzań próbowało łączyć się z serwerami cyberprzestępców, co wskazuje na większą skalę ataku.

Projekt szkodliwego oprogramowania Roaming Mantis może wskazywać, że zostało ono przygotowane z myślą o szerokiej dystrybucji w Azji. Szkodnik obsługuje cztery języki: koreański, chiński uproszczony, japoński oraz angielski. Ślady pozostawione w kodzie przez cyberprzestępców sugerują, że autorzy posługują się głównie językiem koreańskim i chińskim uproszczonym.

Roaming Mantis to aktywne i szybko zmieniające się zagrożenie. Dlatego zdecydowaliśmy się opublikować nasze odkrycia już teraz, nie czekając na zakończenie szczegółowej analizy. Cyberprzestępcy wydają się być mocno zmotywowani, zatem użytkownicy i firmy powinny mieć świadomość zagrożenia. Wykorzystanie przez atakujących zainfekowanych routerów i techniki przechwytywania ustawień DNS to jasny sygnał, że należy przykładać dużą wagę do ochrony sprzętu sieciowego oraz należytego zabezpieczania sieci powiedział Suguru Ishimaru, badacz ds. cyberbezpieczeństwa, Kaspersky Lab.

Produkty Kaspersky Lab wykrywają szkodliwe oprogramowanie Roaming Mantis jako Trojan-Banker.AndroidOS.Wroba.

Aby zabezpieczyć swoje połączenie internetowe przed infekcjami podobnymi do Roaming Mantis, należy wykonać następujące działania:

Zmień domyślny login i hasło do panelu administracyjnego swojego routera.

Upewnij się, że ustawienia DNS w routerze nie zostały zmodyfikowane. Jeżeli nie wiesz, jakie są prawidłowe ustawienia DNS, skontaktuj się ze swoim dostawcą internetu.

Unikaj instalowania w routerze oprogramowania układowego (firmware) pochodzącego od nieautoryzowanych dostawców.

Nie instaluj na urządzeniach z Androidem aplikacji spoza oficjalnych źródeł.

Regularnie uaktualniaj oprogramowanie układowe swojego routera z oficjalnego źródła.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie https://www.kaspersky.pl/nowosci.

Piotr Kupczyk
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kup czyk@kaspersky.pl
Tel. 34 390 94 00

Aktywacja: 16/04/18 11:12, odsłony: 394