Cyberdefence 24

aut. Sylwia Gliwa 04.11.2019

KOLEJNE WYKRYTE ZAGROŻENIE NA ANDROIDA? TAK, ALE JAKŻE INNOWACYJNE

Użytkownicy Androida zapewne nie będą zdziwieni kolejnym wykrytym, złośliwym oprogramowaniem. Tym razem Symantec informuje o aplikacji „Xhelper", która mogła w przeciągu ostatnich 6 miesięcy zainfekować nawet 45 000 urządzeń. Tylko w przeciągu ostatniego miesiąca ofiarami padło 131 urządzeń. Czy cyberprzestępcy zaskoczyli nam czymś innowacyjnym?

Co wyróżnia Xhelper od innych dotychczas wykrytych zagrożeń na Androida? Złośliwa aplikacja jest trwała i potrafi .....zainstalować się ponownie nawet po odinstalowaniu przez użytkownika. Została zaprojektowana tak, aby pozostać w ukryciu i nie pojawiać się podczas uruchamiania systemu. Tym samym oprogramowanie może wykonywać swoje działania w ukryty sposób. Jak podkreśla Symentec w komunikacie, sami użytkownicy bezpośrednio skarżą się na aplikację na forach internetowych, narzekając na wyskakujące reklamy oraz brak możliwości odinstalowania oprogramowania.

Eksperci Symentec informują, że aplikacja ukrywa się, pobiera bez zgody użytkownika inne złośliwe aplikacje oraz wyświetla reklamy. Jej działanie jest ukierunkowane głównie na użytkowników w Indiach, Stanach Zjednoczonych i Rosji.

Aplikacji nie można również uruchomić ręcznie, ponieważ brak jest widocznej ikony aplikacji – podkreśla Symentec. Uruchamia się natomiast przez zdarzenia zewnętrzne – podłączenie/odłączenie od źródła zasilania czy ponowne uruchamianie urządzenia. Oprogramowanie rejestruje się jako „usługa pierwszego planu", dzięki czemu w przypadku braku pamięci zmniejsza się ryzyko jej odłączenia. Aplikacja umożliwia pobieranie dodatkowych szkodliwych narzędzi – dropperów, clickerów i rootkitów. Możliwości są tak ogromne wskazuje Symentec, że umożliwia atakującemu wiele opcji od kradzieży danych po całkowite przejęcie urządzenia.

Eksperci Symentec po raz pierwszy napotkali na aplikację w marcu br., jednak wówczas kod był bardzo prosty i miał na celu odwiedzanie stron reklamowych. Jak podkreślono w komunikacie, oprogramowanie ewaluowało i obecnie wygląda na to, że jego funkcjonalność wciąż nie została w pełni osiągnięta. Po zbadaniu kodu, eksperci sądzą, że potencjalnie kolejnymi ofiarami mogą stać się użytkownicy Jio – największej sieci 4G w Indiach.

Prawdopodobnie złośliwe oprogramowanie jest pobierane z nieznanych źródeł, jak podkreślił Symentec, nie wykryto próbek w oficjalnym sklepie Google. Częściej aplikacja jest instalowana na określonych markach telefonów co pozwala sądzić ekspertom, że agresorzy skupiają się właśnie na tych określonych markach.