**Android: Specjaliści Check Point odkryli potencjalne zagrożenie atakiem Next Generation**

**Bindery, czyli narzędzia umożliwiające zdalny dostęp do danych, narażają urządzenia z systemem Android na kradzież danych i informacji poufnych**

[Check Point® Software Technologies Ltd.](http://www.checkpoint.com/) (Nasdaq: CHKP), światowy lider na rynku zabezpieczeń sieciowych ogłosił wyniki nowej analizy: *Man in the Binder: He Who Controls the IPC, Controls the Droid*.

**Raport, który jest analizą systemu operacyjnego (OS) Android pokazuje, że dane oraz informacje przechowywane na urządzeniach Android mogą być celem ataków hakerów podczas procesu przesyłania IPC (Inter-Process Communication).**

Analitycy firmy Check Point, pracujący w ramach grupy Malware and Vulnerability Research odkryli, iż bindery, ze względu na swą rolę w procesie komunikacji, są podstawowym celem ataków dla złośliwego oprogramowania. W standardowej sytuacji system operacyjny (OS) nawiązuje współpracę z wieloma elementami warstwy sprzętowej systemu komputerowego: twardym dyskiem, adapterem, kartą sieciową… Tymczasem, ze względu na architekturę urządzeń Android, proces ten może przebiegać w sposób podobny jednocześnie będąc kontrolowanym przez bindery. W takiej sytuacji Binder może zostać użyty do przechwycenia poufnych informacji (m.in. tych wprowadzanych z klawiatury lub przesyłanych jako SMS).

*Dzięki badaniu Man in the Binder odkryliśmy wiele wrażliwych punktów systemu IPC instalowanego w urządzeniach Android. Jednym z nich jest zagrożenie w postaci złośliwego oprogramowania malware. Brak świadomości zagrożenia danych wysyłanych za pomocą systemu IPC jest głównym czynnikiem jaki wykorzystują cyberprzestępcy* – podkreśla **Nitay Artenstein**, analityk ds. bezpieczeństwa w firmie Check Point Software Technologies.

*Bez wielopoziomowego systemu zabezpieczeń narażamy się na dostęp cyberprzestępców do wielu aplikacji na naszych urządzeniach.*

**Najważniejsze wnioski:**

- Raport *Man in the Binder* odkrył bardzo duże zagrożenia w komunikacji

pomocą spoiwa łączącego urządzenia z systemem Android;

- Zagrożenie dotyczy zarówno informacji wysłanych jak I odbieranych przez różny

typ urządzeń, włącznie z urządzeniami posiadającymi dwu-poziomowy system szyfrowania lub inne zabezpieczenia;

- Dane, które mogą być wykradzione wykorzystując niezabezpieczone łącza urządzeń mobilnych: ustawienie klawiatury, informacje o transakcjach bankowych, treść wiadomości SMS;

- W świetle w/w informacji firma Check Point zaleca przedsiębiorstwom wprowadzenie wielopoziomowego systemu zabezpieczeń, w celu ochrony systemu Android przed atakami złośliwego oprogramowania.