

## MOBILNY ADWARE JEDNĄ Z NAJCZĘSTSZYCH FORM CYBERATAKÓW?

---

Złośliwe oprogramowanie reklamowe typu adware w smartfonach może nieść ryzyko ataków hakerskich - wynika z raportu firmy Check Point. Szacuje się, że w ubiegłym roku ofiarami tego typu ataków padło 27 proc. firm na całym świecie.

Z analiz firmy Check Point wynika, że oprogramowanie reklamowe w urządzeniach mobilnych, czyli tzw. mobilny adware to jedna z najczęstszych form cyberataków. Ich celem jest kradzież danych osobowych z urządzenia użytkownika. Oprogramowanie tego typu jest zwykle rozpowszechniane za pośrednictwem aplikacji mobilnych. A tych jest sporo, bo jak donosi niemiecki portal internetowy Statista, na rynku istnieje 2,5 mln aplikacji na Androidy i 1,8 mln aplikacji dla urządzeń iOS.

"Mobilny adware to forma złośliwego oprogramowania zaprojektowana do wyświetlania niechcianych reklam na ekranie urządzenia. Może ono być wykorzystywane przez cyberprzestępców m.in. do przeprowadzania cyberataków szóstej generacji. Cyberprzestępcy potrzebują tylko jednego zainfekowanego urządzenia mobilnego, aby ukraść poufne informacje i uzyskać dostęp do wewnętrznej sieci firmy" - mówi Wojciech Głazewski, szef polskiego oddziału Check Pointa.

Jak zauważają eksperci, adware opracowano w taki sposób, żeby był on w stanie niezauważalnie wkraść się do urządzenia. Odinstalowanie wirusa jest niezwykle trudne, a gromadzone przez niego informacje, w tym dotyczące lokalizacji użytkownika, są poważnym zagrożeniem dla prywatności.

Jak podaje Check Point, jednym z przykładów możliwości adware'u jest Agent Smith, czyli wariant mobilnego szkodliwego oprogramowania wykryty w ubiegłym roku przez badaczy firmy. Agent Smith zainfekował około 25 milionów urządzeń mobilnych na całym świecie, jednak nie został zauważony przez użytkowników. Aby pozostać w ukryciu celowo naśladował aplikację Google i wykorzystywał znane luki w zabezpieczeniach systemów Android, automatycznie zastępując zainstalowane aplikacje wersjami zawierającymi złośliwy kod - wszystko bez wiedzy użytkownika. Wykorzystał również zasoby urządzeń, wyświetlając fałszywe reklamy, które mogłyby generować dodatkowy zysk np. poprzez kradzież danych uwierzytelniających banku i podsłuchiwanie.

Szacuje się, że w ubiegłym roku ofiarami tego typu ataków padło 27 proc. firm na całym świecie.