**Check Point: 210 aplikacji gier w Google Play Store zarażonych!**

**Zespół analityków firmy Check Point odkrył bardzo niebezpieczne zjawisko ataku hakerów przez popularne gry, dostępne w Google Play Store. Okazuje się, że w ostatnim czasie 210 gier, pobieranych przez posiadaczy telefonów komórkowych na świecie, padło ofiarą ukrytej kampanii mobilnej. W konsekwencji, użytkownicy telefonów pobrali ponad 147 milionów zainfekowanych aplikacji na swoje urządzenia. Malware nazwany ‘’SimBad’’ powoduje, że telefony wyświetlały ukryte reklamy, bez możliwości ich usunięcia z urządzenia.**

Grupa analityków z Check Pointodkryła kilkanaście aplikacji Android z ukrytym, złośliwym oprogramowaniem w zestawie do zarabiania Software Development Kit (SDK), popularnie nazywanym SWAnalytics. Zestaw ten jest często wykorzystywany przez producentów gier (pozwala na wyświetlanie większej ilości reklam i większe przychody), będąc zintegrowanym z popularnymi aplikacjami na urządzenia Android, oferowanymi przez Chińskich producentów gier i sklepy online. Po pobraniu aplikacji, system SWAnalytics wykrada z telefonu użytkownika dane (lista kontaktów) i przesyła do zdalnego serwera, należącego do hakerów.

Do dziś 12 spośród zainfekowanych aplikacji, z których większość stanowiły aplikacje systemowe, zostało pobrane 111 milionów razy przez użytkowników na całym świecie. Oznacza to, że hipotetycznie hakerzy mogli mieć niepowołany dostęp do listy nazwisk i numerów telefonów 1/3 całej populacji Chin! Bardziej prawdopodobne jest jednak, że dane te krążyły na czarnym rynku i były wykorzystane do uciążliwych działań marketingowych lub skanowania danych.

Analizy zespołu Check Point Research są o tyle niepokojące, że *grupa ryzyka* rośnie z roku na rok…. Jak wynika z danych firmy Sensor Tower, w 2017 roku użytkownicy ściągnęli różnego rodzaju aplikacje ponad 90 mld razy, z czego 64 mld z Google Play i 28 mld z App Store! To wzrost rok do roku o 13,5 proc.

Jednocześnie, wśród aplikacji dostępnych na platformach App Store i Google Play najpopularniejszą kategorią są gry mobilne. W 2018 roku przychody z tego segmentu osiągnęły poziom blisko 50 mld dol. stanowiąc ponad 80 proc. wszystkich wydatków użytkowników przeznaczonych na programy. Użytkownicy App Store w ub.r. wydali na aplikacje 38,5 mld dol. (wzrost o 34,7 proc.), natomiast przychody deweloperów funkcjonujących w Google Play osiągnęły poziom 20,1 mld dol. (wzrost o 34,2 proc)\*

W 2018 roku służby wywiadowcze USA wielokrotnie ostrzegały ([raport](https://www.dni.gov/files/NCSC/documents/news/20180724-ncsc-press-release-foreign-econ-esp-cyber.pdf)), że chińskie firmy stojące za atakami na oprogramowanie bezpieczeństwa łańcucha dostaw stwarza realne zagrożenie dla gospodarki USA.

W przeszłości hakerzy dokonywali już podobnych ataków. W 2017 roku fala ataków hakerskich NotPetya dotknęła setek tysięcy komputerów na całym świecie, w wyniku czego poszkodowane zostały wielkie firmy, instytucje rządowe i osoby prywatne. Podobnie ofiarą ataku padła powszechnie używana aplikacja CCleaner, mająca m.in. zabezpieczać urządzenia przez szkodliwymi programami. Teraz okazuje się, że zagrożenie stanowi oprogramowanie SDK, powszechnie wykorzystywane przez producentów popularnych gier – ostrzegają analitycy **Check Point Research.**

Wprowadzenie wielopoziomowych systemów zabezpieczeń jest rozwiązaniem dla firm przed nasilającymi się atakami złośliwego oprogramowania ukrytego w wielu aplikacjach, dostarczanych przez poddostawców systemów IT. Niestety coraz więcej aplikacji pojawia się w naszym IT ekosystemie, co zwiększa podatność użytkowników urządzeń mobilnych na kolejne ataki.

*\*Dane za Sensor Tower Report 2018*