Gdy cyberprzestępcy ciężko pracują, pracownicy światowych potęg internetowych wypoczywają na wakacjach. Efekt? Największe światowe serwisy internetowe, YouTube oraz iTunes zaatakowane przez żądnych zysku hakerów.

Jabłko toczone przez robaka

Co atrakcyjnego widzi przeciętny haker w serwisie iTunes? Przeciętny haker nie widzi w nim nic specjalnie interesującego. Być może dlatego strona Apple nie została zaatakowana przez przeciętnego hakera, lecz takiego, który dobrze znał się na rzeczy. Świadczy o tym sposób, w jaki zaprojektował swoje działania.
Cyberprzestępca uzyskał najpierw dostęp do znacznej ilości kont użytkowników iTunes, prawdopodobnie za pomocą zręcznie przeprowadzonego ataku phishingowego. Dostęp do kont iTunes oznaczał, że mógł on z łatwością dokonywać zakupów w sklepie Apple. Za każdy zakup ściągana była opłata z kont indywidualnych użytkowników serwisu. Jest to jednak dopiero początek.

Kupował własne aplikacje za cudze pieniądze

Cybeprzestępcy wcale nie chodziło o zakup konkretnych aplikacji ani muzyki. Atak opierał się na czym innym. Oszust kupował… swoje własne aplikacje, które figurowały na stronie sklepu jako aplikacje z działu „książki", lecz w rzeczywistości były złośliwym oprogramowaniem. Kupił ich tak wiele na raz, że w ciągu jednego dnia znalazły się one w kategorii najbardziej popularnych aplikacji do ściągnięcia. Dopiero teraz wydarzyło się to, na co od początku liczył haker. Zwabieni popularnością aplikacji klienci sklepu zaczęli masowo kupować podszywające się pod aplikacje „złośliwe oprogramowanie".
Wszystko zaczęło się w niedzielę, kiedy pracownicy portalu thenextweb.com zdali sobie sprawę z przekrętu. Ich podejrzenia wzbudził fakt, iż 40 z 50 najpopularniejszych aplikacji w kategorii „książki" pochodziły od tego samego wietnamskiego producenta o nazwie „Thuat Nguyen". Dodatkowo, klienci sklepu zaczęli narzekać, że ktoś wkradł się na ich konta, z których dokonał wielu nielegalnych zakupów na sumy od kilku do nawet 600 dolarów.
Apple zareagowało na sytuację usuwając ze sklepu wszystkie aplikacje złośliwego hakera oraz zatrzymując wszystkie niedokończone przepływy pieniężne. Użytkownikom zalecono natychmiastową zmianę hasła na nowe.

Co na to eksperci?

„Sklep Apple jest jednym z tych miejsc, w których o oszustwo nietrudno, ponieważ aplikacje dodawane są przez każdego, kto ma taką ochotę. Sytuacja przypomina tę z aplikacjami na Facebooku. Tak zwane farmy aplikacji stają się szybko bardzo poważnym wyzwaniem dla światowych potentatów internetowych takich jak Apple. Podobny mechanizm wykorzystywany jest przez cyberprzestępców stosujących nielegalne techniki SEO, w nadziei na wzrost popularności swoich stron i wrzucenie ich na pierwszą stronę wyszukiwarki Google. Rada dla kupujących w iTunes i innych podobnych sklepach: kupować aplikacje tylko od zaufanych producentów, co jakiś czas zmieniać hasło i stosować najbardziej aktualne oprogramowanie antywirusowe" – mówi Łukasz Nowatkowski, dyrektor techniczny w firmie G Data Software.

Someday Interactive