NSA i GCHQ kradną klucze szyfrujące do telefonów komórkowych

27 września 2016

Dane dostarczone przez Edwarda Snowdena wciąż przynoszą owoce, jednakże konsekwencje najnowszych wieści są ponure dla każdego, kto choć trochę troszczy się o swoją telefoniczną prywatność.

Według jeszcze niedawno tajnych dokumentów NSA (National Security Agency – Agencja Bezpieczeństwa Narodowego) i jej brytyjski odpowiednik, GCHQ (Government Communications Headquarters – Centrala Łączności Rządowej), prowadzą szeroko zakrojoną operację przeciwko firmie Gemalto będącej jednym z największych na świecie producentów kart sim do telefonów komórkowych.

Aby zrozumieć znaczenie tej wiadomości, warto wiedzieć trochę o tym, jak są wykorzystywane karty sim. W przypadku łączy 3G lub 4G połączenie pomiędzy naszym telefonem i nośnikiem sygnałów telefonicznych jest szyfrowane. To szyfrowanie nie jest doskonałe, niemniej złamanie go nadal jest czasochłonne, szczególnie jeśli celem jest monitorowanie milionów ludzi jednocześnie.

Każda karta sim ma swój unikalny ciąg szyfrujący znany jako „Ki”. Nośniki są dostarczane do sieci razem z kopią każdego Ki, co pozwala sieciom śledzić i uwierzytelniać każde urządzenie. Rozszyfrowanie połączenia między telefonem i siecią jest trudne. Jeśli jednak posiada się Ki, wówczas jest to proste. Jak zauważa witryna The Intercept, produkcja kart sim i kanały ich dystrybucji nigdy nie były tak projektowane, by zapobiec inwigilacji ze strony rządu.

O skali ataku na Gemalto należy przeczytać, aby weń uwierzyć.

Amerykańskie i brytyjskie agencje wywiadowcze dotarły do wybranych pracowników, monitorowały konta na Facebooku i starannie dobierały cele do hakowania – nie dlatego, że ci ludzie rzekomo zrobili coś złego, ale dlatego, że mogli posiadać informacje ułatwiające nielegalną działalność. W tym samym czasie GCHQ z powodzeniem infiltrowało sieć firmową Gemalto, kradnąc dodatkowe informacje i dane Ki.

Wynik? Miliony kluczy kart sim przeznaczonych dla różnych krajów na całym świecie wyciekły do NSA i GCHQ. Konta e-mailowe i na portalach społecznościowych dziesiątków, a może nawet setek, osób zostały rozszyfrowane w celu ułatwienia dalszego szpiegowania.

Same agencje wywiadowcze mocno podkreślają, że te działania są moralne, legalne i uzasadnione, jest jednak mało prawdopodobne, aby dotknięte tym procederem kraje się z tym zgodziły. Należy jeszcze raz podkreślić, że firmy i osoby fizyczne będące obiektem ataku nie były skazane, oskarżone ani nawet podejrzewane o popełnienie przestępstwa. Jedynym powodem takich rażących naruszeń prawa jest stwierdzenie: „Cóż, mieli informacje, które chcieliśmy dostać".

Zawsze istniały prawne różnice pomiędzy sankcjonowanym przez państwo a bezprawnym zachowaniem, jednakże przepaść między drakońskimi karami za stosunkowo drobne przestępstwa hakerskie a aroganckim zachowaniem rządu szybko się poszerza.

Sophia Helena in't Veld, holenderska posłanka do Parlamentu Europejskiego, stwierdziła: „Jeśli nie jesteś w rządzie i jesteś studentem, to za zrobienie czegoś takiego możesz trafić do więzienia na 30 lat".

Klucze bezpieczeństwa oraz produkty firmy Gemalto są wykorzystywane w setkach milionów urządzeń, poczynając od paszportów, a na telefonach komórkowych kończąc. Firma ta ma mnóstwo klientów w każdym kraju Pierwszego Świata. Według jej kierownictwa była zupełnie nieświadoma, że została tak

dokładnie zinfiltrowana przez zagraniczne służby wywiadowcze. Obecnie prowadzi dochodzenie, ale zabezpieczenie jakiegokolwiek międzynarodowego łańcucha dostaw lub sieci będzie wymagało czasu ze względu na zakres i charakter tej kradzieży.

To nie pierwszy przypadek współpracy GCHQ z NSA. Te dwie agencje pracowały razem, żeby zebrać dane z kamer internetowych użytkowników Yahoo. NSA podsłuchiwała wiadomości przesyłane kablowo pomiędzy USA a Wielką Brytanią w celu uzyskania wewnętrznych, nieszyfrowanych połączeń Google'a.

Tłumaczenie: Nexus
Źródło oryginalne: Extremetech.com
Źródło polskie: Wolna-Polska.pl