Rządowa pluskwa nagrywa nie tylko rozmowy

26 czerwca 2014

Jakich narzędzi mogą użyć władze, by podsłuchiwać obywateli? Częściowych odpowiedzi na te pytanie udzielili eksperci od bezpieczeństwa i można dzięki nim zrozumieć, dlaczego Snowden kazał swoim gościom chować telefony do lodówki.

Rok temu gdy świat poznał Edwarda Snowdena, dziennikarze zwrócili uwagę na pewien dziwny zwyczaj whistleblowera. Gdy przyjmował on gości, kazał im chować telefony do lodówki. Niektórzy zgadywali, że Snowden chciał w ten sposób zablokować możliwość wysyłania i odbierania sygnałów radiowych z telefonów. W rzeczywistości mogło chodzić także o stworzenie bariery dla dźwięku.

Snowden najwyraźniej wiedział, że telefon może służyć do podsłuchu nawet wówczas, gdy jego użytkownik o tym nie wie. Władze różnych państw posiadają narzędzia do tego celu, a dostawcą takich „legalnych" narzędzi jest m.in. włoska firma Hacking Team.

Eksperci od bezpieczeństwa zwrócili uwagę na ofertę Hacking Team już w roku 2011, gdy serwis Wikileaks opublikował wyciek opisujący tzw. przemysł inwigilacji. Zazwyczaj o tym nie myślimy, ale różne firmy tworzą narzędzia do inwigilacji i próbują sprzedawać je rządom. Stoją za tym niemałe pieniądze, więc zachęta do rozwijania takich technologii jest duża.

Firma Hacking Team rozwija narzędzie szpiegowskie o nazwie Remote Control System (RCS). Specjaliści od bezpieczeństwa interesują się nim od dawna, a wczoraj dość obszerne materiały na jego temat opublikowali eksperci Kaspersky Lab oraz Citizen Lab.

Okazuje się, że narzędzia Hacking Team mogą służyć do

szpiegowania telefonów z Androidem, iOS, Windows Mobile oraz BlackBerry. Użytkownicy tego szpiegowskiego narzędzia mogą m.in.:

– podsłuchiwać rozmowy, wiadomości SMS, e-mail;

– włączyć mikrofon by słuchać otoczenia;

– aktywować kamerę;

– sprawdzać historie rozmów, odwiedzane strony, notatki, kalendarze;

– zapisywać wpisywane znaki oraz zrzuty z ekranu.

Eksperci z Citizen Lab dotarli do dokumentów, jakie Hacking Team przygotowała dla swoich klientów. Autentyczność tych dokumentów nie jest w pełni potwierdzona, a ich pochodzenie jest niepewne. Jeśli dokument jest autentyczny, zawiera on wiedzę o tym jaka infrastruktura jest potrzebna do inwigilacji oraz jakie są funkcjonalności systemu.

Umieszczenie pluskwy na telefonie wymaga fizycznego dostępu do urządzenia, albo wcześniejszego zainfekowania komputera. W przypadku urządzeń iPhone konieczny jest wcześniejszy jailbreak. Oprogramowanie szpiegowskie stara się działać dyskretnie np. korzysta z sieci Wi-Fi, aby nie zwracać uwagi na wyższy transfer danych.

Z ustaleń Kaspersky Lab wynika, że Polskie służby mogą korzystać z narzędzi Hacking Team. Trzeba jednak podkreślić, że żaden kraj oficjalnie nie przyznał się do stosowania tego narzędzia w celu szpiegowania swoich obywateli. Odkrycia ekspertów pokazują pewne niewątpliwie istniejące możliwości. Musimy tu mieć na uwadze, że istnieją o wiele prostsze i skuteczne metody podsłuchiwania, co ujawniła chociażby afera taśmowa w Polsce.

Najważniejsze w tej sytuacji wydaje się zwrócenie uwagi na fakt, że przemysł inwigilacji naprawdę istnieje i dla władz

różnych krajów stanowi to niezwykłą pokusę. Ta pokusa może się nasilać w momencie, gdy kontrola nad służbami specjalnymi nie jest wystarczająca. Powiedzmy sobie szczerze, że Polska jest jednym z krajów mających ten problem.

Autor: Marcin Maj
Źródło: Dziennik Internautów