Legalne, ale tajne?

15 lipca 2015

Atak na serwery i zabezpieczenia Hacking Team – włoskiej firmy specjalizującej się w oprogramowaniu szpiegującym – uchylił nam drzwi do świata, który polskie i zagraniczne służby najchętniej chowają pod podłogą. Podejmowane przez różne organizacje, w tym Fundację Panoptykon, próby wydobycia informacji od służb o narzędziach, z jakich korzystają, napotykają na niezmienny opór. Wpadka Hacking Team pokazuje, że ta taktyka ma krótkie nogi: jeśli państwo podejmuje kontrowersyjne działania przeciwko obywatelom, wcześniej czy później – w wyniku wewnętrznego wycieku, ataku czy po prostu rzetelnego, dziennikarskiego śledztwa – wyjdzie to na jaw. Korzystając z medialnych doniesień, podsumowujemy, jakie możliwości polskie służby mogły zyskać dzięki usługom Hacking Team i czy było to zgodne z polskim prawem.

NA CO POZWALA REMOTE CONTROL SYSTEM?

Flagowym produktem, który Hacking Team oferowało służbom specjalnym, jest Remote Control System (RCS) [1] – kompleksowa platforma służąca do infekowania a następnie zdalnego i ukrytego kontrolowania urządzeń takich jakich komputery i telefony komórkowe. RCS umożliwia przejęcie kontroli nad wybranym urządzeniem, a następnie utrwalanie wszystkich czynności jego użytkownika. Operator może oglądać odwiedzane przez ofiarę strony, czytać przesyłaną pocztę, słuchać rozmów wykonywanych przez Skype, a nawet przechwytywać wpisywane hasła. Trudno sobie wyobrazić głębszą ingerencję w prywatność użytkownika.

A to jeszcze nie koniec: przeprowadzona przez społeczność hakerską analiza kodu RCS daje podstawy, by sądzić, że to narzędzie umożliwiało również modyfikowanie treści na zainfekowanych urządzeniach, np. podrzucanie fałszywych dowodów. Taka prowokacja, w postaci podrzucenia np. materiału

o charakterze pedofilskim, otwiera służbom szerokie możliwości działania – od zajęcia samego sprzętu, po zatrzymanie właściciela. Na podstawie samej analizy kodu trudno jednak ustalić, czy taka funkcja mogła zostać uruchomiona przez administratorów zarządzających faktycznymi instalacjami RCS. Tym samym nie wiemy, przez kogo i jak była wykorzystywana (o ile w ogóle).

Według ostatnich doniesień, oprogramowanie dostarczane przez Hacking Team miało też umożliwiać śledzenie użytkowników w sieci TOR, która – co do zasady – gwarantuje anonimowość, ponieważ nie jest w niej ujawniany prawdziwy numer IP użytkownika. Strategia Hacking Team nie opierała się na podważaniu zasad, na jakich działa TOR, ale na zastawianiu pułapek na osoby próbujące dostać się do tej sieci – właśnie po to, by móc zainfekować ich urządzenie i śledzić dalsze działania „od wewnątrz”.

CBA KUPUJE LICENCJĘ

Ujawnione dokumenty pozwalają na zrekonstruowanie listy klientów Hacking Team [2]. Są na niej reżimy nie cieszące się dobrą reputacją, jeśli chodzi o przestrzeganie praw człowieka – m.in. Kazachstan, Azerbejdżan, Uzbekistan, Oman, Arabia Saudyjska, Etiopia, Nigeria, Sudan. I jest także Polska. W 2012 r. Centralne Biuro Antykorupcyjne kupiło od Hacking Team licencję za 178 tys. euro, a w kolejnych latach płaciło ponad 35 tys. euro rocznie za wsparcie techniczne. To jednak nie oznacza, że polskie służby mogły korzystać (ani, że w praktyce korzystały) ze wszystkich możliwości, jakie daje RCS.

System składa się z różnych modułów, których funkcje i możliwości różnią się zasadniczo, m.in. w zależności od systemu operacyjnego i typu urządzenia, jakiego dotyczy konkretna licencja. Zakres możliwości technicznych, jakie stwarzała licencja wykupiona przez CBA, nie jest jasny. Wiemy tylko, że pozwalała na zainfekowanie do 10 komputerów, bez możliwości zarażania urządzeń mobilnych.

Z opublikowanych maili wynika, że w 2014 r. CBA rozważała zmianę licencji na taką, która pozwala infekować również urządzenia mobilne, ale nie potwierdzono tej dodatkowej transakcji. Korespondencja między polską służbą i Hacking Team sugeruje, że sposób działania RCS nie był szczególnie przyjazny i polscy administratorzy nie byli z niego zadowoleni. Można zatem przypuszczać, że ta współpraca z czasem została rozwiązana. Z drugiej strony ujawnione dokumenty wskazują na próby sprzedaży systemu RCS innym polskim służbom, ale nie mamy dowodów potwierdzających ewentualne transakcje.

CO NA TO POLSKIE PRAWO?

Zgodnie z obowiązującym prawem, polskie służby – w tym CBA – mogą dość swobodnie korzystać z narzędzi służących do kontrolowania (przechwytywania) komunikacji elektronicznej w sposób niejawny. Przepis, z których wynikają te uprawnienia, został sformułowany na tyle ogólnie, że nie wyklucza zastosowania takiego oprogramowania jak RCS. To jeden z problemów, na które w swoim wniosku do Trybunału Konstytucyjnego zwróciła uwagę Rzecznik Praw Obywatelskich [3]. Niestety, sędziowie stwierdzili, że na poziomie przepisów nie ma potrzeby doprecyzowania uprawnień służb, tak długo jak sądy – wyrażając zgodę na kontrolę operacyjną – jasno wyznaczają jej granice. Praktyka sądowa na tym polu jest bardzo różna, ale jasne wskazanie narzędzia i sposobu, w jaki może zostać wykorzystane, nie należy do standardu. W efekcie decydują prowadzący kontrolę operacyjną agenci. W ramach istniejących uprawnień, na podstawie ogólnie sformułowanej zgody sądu, mogą włamać się na nasze urządzenie, przechwycić hasło do poczty, przeczytać maile czy podsłuchać rozmowę.

Jak pokazała sprawa Beaty Sawickiej, poza ścisłymi ramami tzw. operacji specjalnych, służby nie mogą jednak stosować prowokacji. A zatem, gdyby nawet – dzięki systemowi RCS – CBA zyskało techniczną możliwość podstawiania śledzonym osobom fałszywych dowodów, nie mogłoby z niej skorzystać w granicach

prawa. Operacje specjalne, które prawo dopuszcza w uzasadnionych przypadkach, nie polegają na wrabianiu niewinnej osoby w przestępstwo czy wykroczenie, którego nie popełniła. Kolejny prawny problem związany z możliwościami systemu RCS to ewentualne ujawnianie informacji na temat prowadzonej kontroli operacyjnej samej firmie Hacking Team. Wśród komentatorów ten wątek wzbudza największe kontrowersje: czy dostawcy systemu mogli się dowiedzieć, jak ich narzędzie jest wykorzystywane w praktyce? Nie ma na to twardych dowodów – są tylko spekulacje oparte o elementy kodu (tzw. watermarking).

KONTROWERSJE I OTWARTE PYTANIA

Medialne spekulacje to z pewnością za mało, by czynić polskim służbom zarzut z naruszenia standardów ochrony informacji niejawnych i narażenia obywateli czy samych instytucji państwa na nielegalne szpiegowanie przez włoską firmę. Kierunek tej dyskusji pokazuje jednak możliwe zagrożenia: decydując się na zakup komercyjnych rozwiązań, szczególnie za granicą, polskie służby stają przed poważnym wyzwaniem w postaci zweryfikowania możliwych technicznych haków i dobrego zabezpieczenia swoich interesów. W praktyce nie musi to być proste. Na kanwie tej sprawy wraca też pytanie o etyczne standardy w handlu bronią i szpiegowskim oprogramowaniem. Czy Polska powinna zawierać transakcje z firmami, które de facto wspierają działania autorytarnych reżimów? Jeśli poważnie traktujemy prawa człowieka, dobrą praktyką byłoby bojkotowanie takich dostawców, jako wyraz oficjalnej polityki państwa. Wreszcie, z perspektywy obywateli, nasuwa się pytanie o sens i granice utrzymywania takich transakcji w sferze tajności. Skoro państwo nie widzi potrzeby ukrywania swoich zdolności inwigilacyjnych wobec zagranicznej firmy, dlaczego tak się obawia własnych obywateli?

Kilka tygodni temu zwróciliśmy się do Centralnego Biura Antykorupcyjnego z wnioskiem o udostępnienie informacji publicznej [4] dotyczącej wykorzystywanych narzędzi inwigilacji, która może dotyczyć każdego obywatela. CBA wydało

decyzję odmowną, powołując się na konieczność zachowania tajemnicy w zakresie wykorzystywanych metod i środków pracy. O wykorzystywanie – już konkretnie systemu RCS – pytała też Helsińska Fundacja Praw Człowieka. I tym razem CBA uznało, że jest to informacja niejawna, a sąd administracyjny oddalił skargę organizacji w tej sprawie. Tak długo, jak oficjalna droga do informacji pozostaje zablokowana, jesteśmy skazani na domysły i wycieki.

Czy nie lepiej byłoby, tak jak ma to miejsce w przypadku podsłuchów (których stosowania nikt się nie wypiera, a służby same publikują dane pokazujące skalę ich wykorzystania) czy dostępu do billingów, wprowadzić temat koni trojańskich i innych metod przechwytywania komunikacji elektronicznej w sferę merytorycznej debaty publicznej? Jeśli takie działania są realizowane w granicach prawa, nie ma powodu, by je ukrywać.

Autorstwo: Katarzyna Szymielewicz
Współpraca: Kamil Śliwowski, Wojciech Klicki
Źródło: Panoptykon.org

PRZYPISY

[1]
http://niebezpiecznik.pl/post/czym-rzad-hackuje-telefony-obywateli/

[2]
http://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech
https://zaufanatrzeciastrona.pl/post/nie-tylko-cba-abw-skw-i-cbs-rowniez-zainteresowane-konmi-trojanskimi/

[3]
https://panoptykon.org/wiadomosc/czy-sluzby-moga-nas-kontrolowac-np-za-pomoca-gps-wniosek-rpo-do-trybunalu-konstytucyjnego

[4]

https://panoptykon.org/wiadomosc/perypetie-zbierania-informacji