

Telefony komórkowe i ich tajemnicze zastosowanie

23 sierpnia 2013

Każdy korzysta na co dzień z funkcji jakie oferują współczesne telefony komórkowe. Lecz nie każdy jest świadom ich „drugiej” funkcjonalności. Oczywiście nie każdy z nas jest premierem czy prezesem korporacji aby opisane techniki były skierowane przeciw niemu, ale warto wiedzieć jak gromadzi się informacje i jakie dają możliwości analityczne.

Na początku informuję, iż mam na myśli nie tylko współczesne telefonyw komórkowe, topowe samartfony, ale również wiekowe „cegły” używane np. przez prezydenta Lecha Kaczyńskiego (nie bez powodu „staroświecki prezydent bez konta bankowego” otrzymał od swych doradców staroświecki model).[1]

Popularne telefony są obsługiwane przez różne systemy operacyjne, np.: Windows Mobile, Symbian, Android, Blackberry, Windows Phone 7, Bada itp. Oferujących szeroką funkcjonalność dla użytkowników dzięki czemu przypominają dziś bardziej komputery niż telefony czasów moich rodziców. Co z tego wynika?

Zainstalowana i działająca na telefonie aplikacja może sfotografować twoje otoczenie, zrobić jego model w 3D z taką dokładnością, że dokumenty leżące na biurku można odczytać. Krótki opis złośliwej aplikacji PlaceRaider działającej w tle bez wiedzy użytkownika na systemie Android (obudowany Linux) można znaleźć w internecie.[2] Jak widać sam użytkownik może zainstalować tą lub inną aplikację o podwójnym działaniu nie wiedząc o tym.

Czytając powyższe już wiesz, że należy dokładnie przyjrzeć się temu, co instalujesz na telefonie (komputerze). Jeśli ustrzegliśmy się złośliwej aplikacji/wirusa dzięki własnej ostrożności – to świetnie! Lecz pole do popisu posiadają

również producenci telefonów (z własnej woli lub nakazów państwowych instytucji). Fabrycznie instalowany trojan Carrier iQ zapisuje wciskane klawisze np. w trakcie szyfrowanej sesji podczas logowanie się do poczty e-mail, czyli nasze hasło i login (typowy keylogger[3]). W USA 140 milionów telefonów posiada te oprogramowanie – co przyznaje producent.[4]

Cóż, mamy pecha jeśli posiadamy któryś z tych telefonów. Więc czy wybierając inny model komórki oraz operatora możemy czuć się bezpiecznie? Nasze położenie oraz droga, którą przebyliśmy jest stale rejestrowana przez aplikacje lub operatorów.[5] Lokalizując w ten sposób np.: sprawcę fałszywych alarmów bombowych[6], dzieci[7], swoich pracowników[8], znajomych[9], zgubiony aparat[10]. Poprzez unikalny numer identyfikacyjny telefonu IMEI i karty sim USIM/ISIM, wyliczenie odległości od 2-3 różnych nadajników (niekoniecznie tego samego operatora – BTS[11]), dane z nawigacji GPS. Idea świetna lecz należy pamiętać, że każdy z operatorów musi przekazać tego typu informacje służbom państwowym na ich żądanie. A czy na pewno do tego typu (i innych) interwencji potrzebny jest nakaz sądowy?

„Rozporządzenie Rady Ministrów z września 2005 roku nakazuje operatorom telekomunikacyjnym udostępniać „ABW i Policji system zapewniający niezależny dostęp do treści przekazu telekomunikacyjnego”. To oznacza, że służby mają otwarty dostęp do telefonicznych baz danych, bez udziału operatora. Mało tego służby specjalne, także bez wiedzy operatora, mogą podłączać się np. do studzienek telefonicznych i podsłuchiwać nasze rozmowy.”[12]

Ponadto w branży telekomutacyjnej nie jest tajemnicą, iż u każdego z operatorów pracują na pełnym etacie tacy analitycy. „Art. 179 ust. 4b prawa telekomunikacyjnego mówi, że teleoperatorzy powinni udostępniać dane ”bez udziału pracowników przedsiębiorcy telekomunikacyjnego”. W praktyce: przedstawiciele służb mają swoje własne “pokoje” u teleoperatorów z nielimitowanym dostępem do ich baz danych.

Można się zatem domyślić, jak wygląda “kontrola” pracy takiego pracownika służb (a raczej jej brak). Potwierdza to cytowany w artykule Siedleckiej[13] Wacław Iszkowski, prezes Polskiej Izby Teleinformatyki.”[14] „Leniwi” analitycy mogą po prostu „poprosić” o odpowiednie dane, co robią często.

Powątpiewasz w wierność małżonka? Oferta weryfikująca ją jest dość szeroka dla przeciętnego Kowalskiego – SpyPhone dla każdego.[16] Przecież służby nie będą nam niczego instalować (nie licząc fabrycznych backdoorów[17]) bo po co?. W pierwszej kolejności pan z pokoju powyżej sprawdzi nasze bilingi oraz treści SMS-ów, które każdy operator ma obowiązek przechowywać minimum 2 lata.[18]

Grzebanie w archiwum to nie pełen wachlarz możliwości operatorów telekomunikacyjnych. Przypominają mi się reklama polskiego operatora Play, wówczas wchodzącego na rynek i borykającego się z problemem dobrego pokrycia sygnałem kraju. Kampania miała to zmienić. Spot blisko 30 sekundowy przemycił ciekawy fakt. Spotkanie mafijnych gangsterów przy stole w pewnej chatce na odludziu. Przed rozmową na hasło ojca chrzestnego wszyscy wyjmują telefony komórkowe, wyłączają i wyjmują baterię. Do jednego z nich zwraca się ojciec mówiąc: „Ty nie musisz, jesteś w Play”. Śmiech pozostałych.

Wyłączają telefony gdyż: operator/złośliwa aplikacja może zdalnie włączyć w naszym telefonie np. mikrofon i słuchać (w tym nagrywać) wszystkiego co dzieje się wokół.[19, 20] Świadomy „gangster” wyłącza telefon i może czuć się bezpiecznie? Nie! Telefon wyłączony również można podsłuchiwać! Więc najlepszym rozwiązaniem jest wyjęcie baterii (fizyczne odcięcie zasilania) i wyjęcie karty SIM.[21]

„Z trudem i po wielkich bojach udało się przekonać członków rządu, by nie zabierali telefonów komórkowych na salę obrad, mimo że – jak twierdzą specjaliści z pionu operacyjnego UOP – podsłuchiwać można nawet wtedy, gdy telefon jest wyłączony. Uniemożliwia go dopiero rozłączenie baterii.”

Już wiecie dlaczego w sejmie przed drzwiami sal konferencyjnych stoi ochroniarz z komodą, do której uczestnicy obrad deponują telefony.

Dziś producent m.in. „bezpiecznych” telefoów BlackBerry desperacko szuka inwestorów.[22] Najwyraźniej spór o bezpieczeństwo danych nie wyszedł im na zdrowie.[23] To chyba dobra nauczka dla pozostałych producentów.[24]

Owa druga funkcjonalność może mieć również podłoże komercyjne, bodajże gdy Orange wchodziło do Polski (konkurencja) nagłośniła się w prasie branżowej sprawa „uszkadzania” telefonów klientów na południu Europy pod koniec trwania ich umowy. Usterki były proste, począwszy od niedziałających klawiszy, poprzez miganie ekranu, do resetowanie się, wyłącznie telefonu.

Osobiście wykonałem kawał kilku znajomym wysyłając SMS przy pomocy aplikacji do spoofingu (podszywania się pod nadawcę).

Pomysłów „organom ścigających przestępczość” ciągle przybywa, np.: brak możliwości anonimowego zakupu telefonu (nie licząc kamery w sklepie, unikalnego numeru aparatu).[25] Pociuszające jest tylko to, że do USA jeszcze sporo nam brakuje (analiza szyfrowanych faksów, masowy monitoring, itp.).[26]

Niestety jest to wierzchołek góry lodowej ale warto chociaż go zdobyć aby być świadom swojej anonimowości. Zapraszam do dyskusji w komentarzach.

Autor: kbps

Nadesłano do „Wolnych Mediów”

PRZYPISY

[1] <http://www.naszdziennik.pl/polska-kraj/49120.html>

[2]

<http://niebezpiecznik.pl/post/telefon-szpieg-ukradkiem-sfotografuje-twoj-dom-zrobi-z-niego-model-w-3d-i-pokaze-zlodziejowi/>

[3] <http://pl.wikipedia.org/wiki/Keylogger>

[4]

<http://niebezpiecznik.pl/post/wiekszosc-telefonow-komorkowych-na-podsluchu/>

[5]

<http://niebezpiecznik.pl/post/iphone-i-ipad-zapisuja-gdzie-byles/>

[6]

<http://wiadomosci.wp.pl/kat,1342,title,Ekspert-o-alarmach-bombowych-jest-wiele-sposobow-namierzenia-sprawcow,wid,15763474,wiadomosc.html>

[7]

<http://www.plus.pl/indywidualna/Uslugi/AktualniKlienci/WiemGdzieJestes/>

[8]

<http://www.orange.pl/kid,4000378054,id,4002010406,title,Gdzie-Oni-Sa-,article.html>

[9]

<https://play.google.com/store/apps/details?id=com.fsp.android.friendlocator&hl=pl>

[10]

<https://play.google.com/store/apps/details?id=com.androidlost>

[11]

<http://detektywistyka.rubikon.pl/inwigilacja-gsm-stop.html>

[12]

<http://media2.pl/telekomunikacja/69760-Sluzby-pobieraja-dane-bez-wiedzy-operatorow.html>

[13]

http://wyborcza.pl/1,75968,10898325,Zagladaja_nam_w_SMS_y_.html

[14]

<http://niebezpiecznik.pl/post/sluzby-czytaja-nasze-sms-y-jak-zabezpieczyc-sie-przed-inwigilacja/>

[15]

http://www.isoc.org.pl/system/files/Sprawdzenia_u_operator%C3%B3w.pdf

[16]

<http://www.spyeye.pl/index.php/cPath/74?osCsid=60323fe1cecad607a03467b63b91f6d2>

[17]

<http://zaufanatrzeciastrona.pl/post/backdoor-w-telefonie-zte/>

[18]

http://wyborcza.pl/1,76842,11145078,Jak_dluogo_operatorzy_maja_trzymac_twoje_billingi_i.html

[19]

http://online.wsj.com/article_email/SB10001424127887323997004578641993388259674-lMyQjAxMTAzMDAwMTEwNDEyWj.html

[20]

<http://mobtech.interia.pl/systemy-operacyjne/android/news-fbi-moze-aktywowac-glosnik-w-smartfonie-i-nagrywac-rozmowy,nId,1005791>

[21] <http://www.wprost.pl/ar/?0=8039&C=57>

[22]

http://wyborcza.biz/biznes/1,101562,14436972,BlackBerry_szuka_pomocy_na_zewnatrz.html

[23]

<http://www.komputerswiat.pl/nowosci/internet/2010/31/arabowie-kontra-blackberry-rim-sie-nie-ugnie.aspx>

[24]

<http://niebezpiecznik.pl/post/apple-rim-i-nokia-umiescily-back>

dora-w-swoich-telefonach-na-prosbe-indyjskiego-wywiadu/

[25]

<http://wpolityce.pl/wydarzenia/32085-sluzby-specjalne-chca-polozyc-reke-na-pre-paidach-niebawem-anonimowy-zakup-komorki-moze-stac-sie-niemozliwy>

[26]

<http://zaufanatrzeciastrona.pl/post/usa-monitoruja-na-masowa-skale-rozmowy-telefoniczne-obywateli/>