Kto i jak kontroluje internet

14 lutego 2012

Margaret Coker, dziennikarka Wall Street Journal, która po upadku Trypolisu obejrzała tamtejszy ośrodek podsłuchowy, zauważyła, że wszystko tam było kontrolowane przez satelity: sieć internetowa, telefony komórkowe, połączenia (internetowe i telefoniczne). W teczkach można było znaleźć m.in. e-maile i fragmenty rozmów telefonicznych opozycjonistów rządu Muammara Kaddafiego.

Na ścianie ośrodka znajdowała się tabliczka z logiem przedsiębiorstwa, które założyło całą instalację: Amesys, filia francuskiego koncernu informatycznego Bull [1]. Nieco później Le Canard Enchaîné ujawnił, że dyrekcja wywiadu wojskowego (DRM) pomagała w kształceniu libijskich podsłuchiwaczy [2].W Syrii rząd Baszara al-Asada korzysta z pomocy spółek amerykańskich przy cenzurowaniu Internetu oraz przejmowaniu loginów i haseł swoich obywateli, by mieć dostęp do ich poczty elektronicznej, kont na Facebooku czy Twitterze. To bardzo skuteczne narzędzie poznania wewnętrznych i zagranicznych kontaktów opozycjonisty.

MNIEJ UPRZEJMA WERSJA INTERNETU

Używane technologie noszą łagodną nazwę „Deep Packet Inspection" (DPI, „Głęboka Inspekcja Pakietów"). Kiedy wysyłamy elektroniczny list, dziesiątki maszyn przekazują go kolejno dalej, aż do odbiorcy, zadowalając się odczytaniem adresu. Nie obchodzi ich zawartość przesyłki. Jak wyjaśnia specjalista prawa internetowego, Jonathan Zittrain, „to jak na imprezie pełnej uprzejmych osób. Jeśli stoicie daleko od baru, a jest za dużo ludzi, by doń dotrzeć, prosicie sąsiada, by przekazał prośbę o piwo. Ten prosi z kolei swego sąsiada stojącego trochę bliżej baru, itd. W końcu wasza prośba trafia do baru i piwo wraca tą samą drogą. Wszyscy są dobrze wychowani, więc podczas całej tej operacji nikt nie napił się

waszego piwa” [3].

Jednak w przypadku DPI mamy do czynienia z inną wizją Internetu, mniej uprzejmą. Co byście powiedzieli, gdyby wasz sąsiad z imprezy zaczął analizować waszą prośbę i prawić wam morały? Albo gdyby zmienił zawartość waszej szklanki na wodę, albo wprost przeciwnie – coś dużo bardziej euforyzującego niż piwo? Na to właśnie pozwalają technologie DPI: umożliwiają bowiem czytanie korespondencji, modyfikowanie jej, wysłanie gdzie indziej…

Amesys to niejedyna taka spółka na rynku. Qosmos, inne francuskie przedsiębiorstwo, znalazło się na widelcu Bloomberga. Amerykańska agencja prasowa ujawniła właśnie, że spółka dostarczyła sondy DPI konsorcjum, które ekwipuje Syrię tak samo, jak niegdyś Libię Kaddafiego [4]. W Chinach rozwinięte na Zachodzie technologie DPI tworzą trzon „zapory ogniowej”, pozwalającej rządowi cenzurować korespondencję i szpiegować obywateli.

Jak wskazują liczne dokumenty wewnętrzne tych spółek ujawnione ostatnio przez WikiLeaks, kontrola sieci komunikacyjnych jest „nową, tajną gałęzią przemysłu obsługującą 25 państw. (…) W tradycyjnych historiach szpiegowskich agencje takie jak brytyjska MI5 zakładają podsłuch jednej czy dwóm osobom. W ciągu ostatnich 10 lat normą stały się systemy kontroli masowej” [5]. Nieco wcześniej Wall Street Journal opublikował ponad 200 dokumentów marketingowych 36 spółek proponujących różnym amerykańskim władzom antyterrorystycznym narzędzia do elektronicznej kontroli i piractwa [6].

PATRZ JASNO, DZIAŁAJ SZYBKO

W Stanach Zjednoczonych technologie DPI przeżywały swoje dni chwały w maju 2006 r. Ciszę przerwał Mark Klein, były technik AT&T (wielki dostawca Internetu). Ujawnił, że jego były pracodawca zainstalował w sercu amerykańskiego Internetu produkty spółki Narus. Zleceniodawcą była słynna National

Security Agency (NSA), która od przełomu lat 1980. i 1990. zarządza projektem globalnych podsłuchów Echelon. Dewiza Narusa to „See Clearly. Act Swiftly” (Patrz jasno. Działaj szybko). Przedsiębiorstwo edycji technik DPI zostało założone w 1997 r. W 2006 r. 150 jego pracowników zarobiło 30 mln dolarów. W 2010 r. spółkę przejął Boeing. Produkty firmy zostały zainstalowane m.in. w Egipcie, w czasach Hosni Mubaraka [7].

Operatorzy telekomunikacyjni widzą strony internetowe, pocztę elektroniczną, czaty w czasie rzeczywistym, rozmowy na żywo, wideo, listy dyskusyjne, wszelkie dane. Większość tych informacji przepływa jawnie, bez szyfrowania. Jest więc dość łatwo kontrolować użytkowników – zarówno przez niedzielnego hakera, jak i państwowe służby bezpieczeństwa.

Ale i prywatne przedsiębiorstwa mogą być zainteresowane tymi technologiami. Niektórzy operatorzy telekomunikacyjni, tacy jak Free, SFR czy Orange, zaczynają narzekać, że przez ich sieci przepływają masy danych od użytkowników niepłacących za ten transport. Na przykład dostawcy Internetu nie chcą płacić za wideo z Youtube’a, które muszą dostarczać swoim abonentom. Stąd pomysł na wystawianie faktur emitentom danych i odbiorcom oraz selektywnego spowolnienia niektórych rodzajów przekazów, by uprzywilejować inne. Żeby to jednak zrobić, trzeba precyzyjnie wiedzieć, co właściwie przepływa.

Podobnie operatorzy telefonii komórkowej postanowili dostarczać ograniczony akces do Internetu, by zmniejszyć koszty infrastruktury. Utrudniają więc użytkownikom „inteligentnych” telefonów wymianę plików, zmuszając w ten sposób do korzystania z narzędzi komunikacji wokalnej lub wideo – np. Skype’a.

To właśnie technologie DPI pozwalają kontrolować przepływ informacji i zarządzać nim, przyznawać szersze i szybsze łącza wybranym serwisom (np. tym, które operatorzy sami emitują…). To sprzeczne z „neutralnością sieci”, polegającą na tym, że

dostawca dostępu musi przekazywać wszelkie dane, bez żadnej dyskryminacji.

DPI zastosowane do nawigacji w Internecie pozwala zachować ślad wszystkiego, co tam robicie. Specjaliści od marketingu zacierają ręce i marzą, by wykorzystać te dane. Orange niedawno zaproponował swoim klientom usługę opierającą się na DPI, która za zgodę użytkownika na analizowanie jego ruchów w sieci proponuje podsuwanie ściśle dopasowanych do niego ofert handlowych. Po prostu dostawcy Internetu chcą być równie zyskowni, co Facebook i Google. Oczywiście pod warunkiem, że te programy fidelizacji i kontroli przyciągną abonentów; wystarczy jednak głosić, że dane nie będą nikomu przekazywane, by taką formułę w końcu sprzedać.

Zainteresowany czytelnik może zajrzeć na stronę „Data privacy" na witrynie internetowej GFK, międzynarodowej grupy badań marketingowych, akcjonariusza spółki Qosmos. Strona ta mówi jedynie o wykorzystaniu banalnych cookies przeglądarek, ale zapomina wspomnieć, że do śledzenia ruchów internautów używa również technologii DPI, podobno „na zasadzie anonimowości", według tylko sobie znanej recepty. GFK jest obecna w niemal 150 krajach, nie tylko w wielkich demokracjach…

DPI przyciąga także przedsiębiorstwa posiadające prawa i copyrighty. Przedsiębiorstwa te chcą walczyć z „nielegalną" wymianą plików w sieciach wykorzystujących protokół BitTorrent oraz na stronach bezpośredniego ładowania – typu Megaupload. Precyzyjną wiedzę o tym, który internauta próbuje ściągnąć dany film lub plik muzyczny (potrzebną do blokady dostępu) można zdobyć wyłącznie za pomocą „głębokiej" infrastruktury, zainstalowanej w węzłach wymiany danych, czyli u dostawców Internetu.

TEST W WARUNKACH BOJOWYCH

Inny naturalny rynek DPI dotyczy kontroli legalnej. Policja, w ramach śledztwa pod kontrolą sądu czy, jak we Francji,

„Komisji Kontroli Podsłuchów Bezpieczeństwa”, potrzebuje czasem podsłuchać, co mówi jakaś osoba. To jednak rynek niszowy, związany z bardzo małą częścią społeczeństwa. Przedsiębiorstwa z omawianego sektora okazji do zysków muszą więc szukać gdzie indziej.

I to tutaj pojawiają się rządy państw policyjnych, pragnące podsłuchiwać całą ludność. Dzięki tym krajom programy kontroli Internetu są testowane „w warunkach bojowych”. Tunezja w czasach prezydenta Zin Al-Abidina Ben Alego korzystała z rabatów na systemy podsłuchowe, które nie były jeszcze doskonałe. Co do Amesys – Libia stanowiła znakomity poligon doświadczalny dla programu Eagle [8]. Alcatel prowadzi podobne testy w Birmie [9]. Po nitce do kłębka, wykorzystanie danych zebranych przez DPI ułatwia aresztowania i nierzadko tortury.

Parlament Europejski, prawdopodobnie zaintrygowany masową obecnością europejskich przedsiębiorstw na takich rynkach, przyjął rezolucję, której celem jest zakaz sprzedaży za granicę systemów kontroli Internetu, jeśli są one sprzeczne z zasadami demokracji, wolności słowa i praw człowieka [10]. 1 grudnia 2011 r. Rada Unii Europejskiej w ramach sankcji przeciw reżimowi syryjskiemu zabroniła również „eksportu ekwipunku i programów komputerowych przeznaczonych do kontroli Internetu i rozmów telefonicznych”.

Niemniej jednak, eksport produktów do masowego podsłuchu jest bardzo słabo obwarowany prawem. Producenci łatwo omijają przeszkody, gdyż prawodawstwo w tym względzie pozostaje bardzo różne w zależności od kraju. Zezwolenia udzielane przez rządy z reguły nie są publikowane. A programy komputerowe tego rodzaju nie są uważane za broń sensu stricto.

Autor: Antoine Champagne
Tłumaczenie: Jerzy Szygiel
Źródło: Le Monde diplomatique – edycja polska

PRZYPISY

[1] Paul Sonne, Margaret Cocker, „Firms Aided Libyan Spies”, The Wall Street Journal, Nowy Jork, 30 sierpnia 2011.

[2] „Des experts des services secrets français ont aidé Kadhafi à espionner les Libyens”, Le Canard enchaîné, Paryż, 7 września 2011, i „Secret militaire sur le soutien à Kadhafi”, 12 października 2011.

[3] Jonathan Zittrain, „The Web as random acts of kindness”, konferencja TED, lipiec 2009.

[4] „Syria Crackdown Gets Italy Firm’s Aid With U.S.-Europe Spy Gear”, Bloomberg, 3 listopada 2011.

[5] WikiLeaks, „The Spy Files”, 1 grudnia 2011.

[6] Jennifer Valentino-Devries, Julia Angwin, Steve Stecklow, „Document Trove Exposes Surveillance Methods”, The Wall Street Journal, 19 listopada 2011.

[7] Timothy Karr, „One U.S. Corporation’s Role in Egypt’s Brutal Crackdown”, The Huffington Post, 28 stycznia 2011.

[8] Zob. dossier Amesys na Reflets.info.

[9] Diane Lisarelli, Géraldine de Margerie, „Comment Alcatel se connecte à la junte birmane”, Les Inrockuptibles, Paryż, 26 marca 2010.

[10] „Le Parlement européen interdit la vente de technologies de surveillance aux dictatures”, Fhimt.com, 11 października 2011.