XKeyscore wie o Tobie wszystko

2 sierpnia 2013

Edward Snowden ujawnił kolejne narzędzie wykorzystywane przez NSA do inwigilacji. Tym razem dowiadujemy się o istnieniu najprawdopodobniej najpotężniejszego programu tego typu – XKeyscore. Pozwala on na nieautoryzowany dostęp i przeszukiwanie olbrzymich baz danych zawierających e-maile, zapisy czatów i historie surfowania po sieci milionów osób. To najszerzej rozpowszechnione narzędzie inwigilacyjne w internecie.

Na początku czerwca, podczas pierwszej rozmowy przeprowadzonej z dziennikarzem „Guardiana", Edward Snowden stwierdził: „Siedząc przy własnym biurku mogę podsłuchiwać każdego. Od ciebie i Twojego księgowego po sędziego federalnego czy prezydenta. Wystarczy że mam adres e-mail. Teraz, dzięki ujawnieniu XKeyscore wiemy, o czym Snowden mówił. Władze USA zaprzeczały wówczas jego słowom. Mike Rogers, przewodniczący komitatu wywiadu Izby Reprezentantów stwierdził: On kłamie. To niemożliwe by mógł to robić."

Jednak ujawnione teraz przez Snowdena materiały szkoleniowe pokazują, że wypełniając prosty formularz na ekranie komputera pracownik NSA może – bez pytania o zgodę sądu czy konieczności autoryzacji swoich działań u jakiegokolwiek innego pracownika NSA – przeszukać olbrzymią bazę danych z podsłuchu. Jeden ze slajdów szkoleniowych dotyczących XKeyscore mówi, że nadzoruje on „niemal wszystko, co typowy użytkownik robi w internecie". Przechwytuje zarówno metadane jak i zawartość e-maili, witryn internetowych czy pytań zadawanych wyszukiwarkom. Co więcej XKeyscore daje możliwość śledzenia poczynań użytkownika niemal w czasie rzeczywistym.

Zgodnie z amerykańskim prawem do przechwycenia komunikacji

obywatela konieczna jest indywidualna zgoda sądu. XKeyscore pozwala na szeroką inwigilację bez wcześniejszej autoryzacji. Wystarczy, że pracownik NSA zna adres IP lub e-mail interesującej go osoby. Oprogramowanie na bieżąco zbiera dane i daje do nich ciągły dostęp. Analitycy mogą wyszukiwać interesujących ich ludzi po numerze telefonu, adresie, nazwisku, słowach kluczowych, używanym języku czy typie przeglądarki. Analitycy mający dostęp do XKeyscore są uczeni, że wykorzystywanie pełnej bazy danych dostarczy im zbyt wielu trafień, zatem najpierw powinni używać metadanych i na ich podstawie zawężać obszar poszukiwań.

Program XKeyscore wyposażony jest w dodatki zwiększające jego funkcjonalność. Ze slajdu „Plug-ins" z grudnia 2012 roku dowiadujemy się, że możliwe jest „przeglądanie dowolnego adresu e-mail zarówno pod kątem nazwy użytkownika jak i domeny, dowolnego numeru telefonu, aktywności na czacie czy w mailu pod kątem nazwy użytkownika, listy znajomych, ciasteczek specyficznych dla danego komputera itp."

Analityk, który chce przejrzeć e-maile dowolnej osoby, musi jedynie w formularzu wpisać jej adres, okres dla jakiego wyszukuje oraz w polu z uwagami uzasadnić, dlaczego przegląda te maile. Po chwili otrzymuje spis e-maili i zaznacza te, które chce odczytać.

Niezwykle łatwe jest też samo rozpoczęcie inwigilacji. Dodanie konkretnej osoby do zestawu śledzonych wymaga jedynie wybrania kilku pozycji z menu, opisujących podstawy prawne dla inwigilacji oraz uzasadniających ją z punktu widzenia wywiadowczego.

XKeyscore to część sieci wywiadowczej zwanej Digital Network Intelligence (DNI). Jednym z dostępnych narzędzi jest DNI Presenter, który w połączeniu z XKeyscore pozwala na odczytanie prywatnych wiadomości i czata z Facebooka. Aby uzyskać dostęp do takich danych analityk musi wpisać jedynie nazwę konta na Facebooku i interesujący go zakres dat. Jeden

ze slajdów szkoleniowych wyjaśnia: „Dlaczego interesuje nas protokół HTTP? Gdyż niemal wszystko, co typowy użytkownik robi w internecie jest wykonywane za pośrednictwem HTTP.” Na slajdzie tym widać logo Facebooka, Twittera, CNN, Wikipedii czy Gmaila.

XKeyscore pozwala też na określenie adresu IP każdej osoby, która odwiedzi dowolną interesującą NSA witrynę. Ze slajdów dowiadujemy się, że każdego dnia do bazy XKeyscore trafia 1-2 miliardów rekordów zawierających e-maile, wykonywane połączenia telefoniczne i inne rodzaje komunikacji.

XKeyscore zbiera tak gigantyczną ilość informacji, że nie mieszczą się one w centrach bazodanowych. Dlatego też treść komunikacji przechowywana jest średnio przez 3-5 dni, a metadane przez 30 dni. Z jednego ze slajdów dowiadujemy się: „W niektórych miejscach ilość zbieranych danych (ponad 20 terabajtów dziennie), jest tak wielka, że możemy je przechowywać jedynie przez 24 godziny.” NSA rozwiązała ten problem tworząc wielowarstwowy system, dzięki któremu interesujące ją dane są przechowywane w osobnych bazach danych. W jednej z nich, zwanej Pinewale, są przechowywane nawet przez pięć lat.

Zgodnie z prawem podsłuchiwanie obywateli USA wymaga za każdym razem uzyskanie indywidualnego nakazu. Prawo jednak pozwala na nieograniczone podsłuchiwanie obywateli innych krajów. Jameel Jaffer, dyrektor ds. prawnych w ACLU (Amerykańska Unia Wolności Obywatelskich) mówi, że rządzący przyjęli takie przepisy po to, by móc inwigilować własnych obywateli. „Rząd nie musi teraz brać na celownik Amerykanów, by zbierać dane z ich komunikacji. Śledzi komunikację Amerykanów biorąc na cel obywateli obcych państw” – stwierdził.

Co prawda od czasu do czasu przełożeni analityków dokonują audytu ich poczynań jednak, jak mówi Snowden, „bardzo rzadko się zdarza by działania te zostały zakwestionowane”.

Z ujawnionych dokumentów wynika też, że do roku 2008 dzięki XKeyscore udało się złapać 300 terrorystów.

Autor: Mariusz Błoński
Na podstawie: Guardian
Źródło: Kopalnia Wiedzy