Sieć Tor wcale nie taka bezpieczna

17 listopada 2014

Sieć Tor nie jest tak bezpieczna, jak miała być. Europejskie i amerykańskie organa ścigania przeprowadziły akcję „Onyomous", w ramach której przejęły kontrolę nad 27 węzłami sieci Tor i zlikwidowały ponad 400 serwisów. Śledczy nie ujawnili, w jaki sposób ustalili lokalizację wspomnianych węzłów. Architektura sieci Tor powinna uniemożliwiać takie działania.

„W liberalnych demokracjach możemy się spodziewać, że gdy wskutek akcji prowadzącej do zatrzymania i oskarżenia 17 osób, policja powinna wyjaśnić sądowi, w jaki sposób dotarła do podejrzanych. Powinien na tym skorzystać Tor, gdyż zdobędzie w ten sposób wiedzę o ewentualnych dziurach bezpieczeństwa w serwisach korzystających z tej sieci. Tor jest najbardzej zainteresowany zrozumieniem, w jaki sposób zlokalizowano te serwisy i czy oznacza to, iż w sieci istnieją dziury pozwalające na zaatakowanie jej przez cyberprzestępców lub tajne policje represjonujące dysydentów" – oświadczyli przedstawiciele projektu tor.

Wśród zamkniętych serwisów jest Silk Road 2.0. O jego poprzedniku, Silk Road, informowaliśmy już w przeszłości. Zatrzymano też mieszkańca Kalifornii, Blake'a Benthalla, którego oskarżono o uruchomienie Silk Road 2.0.

Władze sugerują, że Benthall został złapany dzięki temu, iż popełnił błąd, gdyż zarejestrował serwer używając do tego celu prawdziwego adresu e-mai. Przedstawiciele Tor sceptycznie podchodzą do tych informacji. Twierdzą oni, że amerykańskie agendy rządowe korzystają ze stworzonej przez siebie konstrukcji prawnej, która pozwala ujawnić nie w jaki sposób zlokalizowały osobę podejrzaną, ale w jaki sposób mogły to zrobić.

Zdaniem przedstawicieli Tora w protokole mogą istnieć jakieś niedociągnięcia, które wykorzystali śledczy. „Wskazuje na to liczba przejętych węzłów i zlikwidowanych serwisów”, oświadczyli.

Jednak specjalista ds. bezpieczeństwa, Luther Martin z Voltage Security, zauważa, że organa ścigania „jedynie zadrapały powierzchnię „ciemnej sieci”, w której działają cyberprzestępcy. Wszystkie serwisy, które zlikwidowano w ramach operacji Onyomous to witryny, które istniały na pierwszym i drugim poziomie ciemnej sieci. Tamtejsze serwisy nie są co prawda indeksowane przez wyszukiwarki, ale są łatwo dostępne dla wszystkich. Wydaje się, że cyberprzestępcy działający na głębszych poziomach pozostali bezpieczni. A to właśnie tam przechowuje się i sprzedaje ukradzione dane o numerach kart płatniczych czy dane medyczne” – stwierdził.

Autor: Mariusz Błoński
Na podstawie: V3
Źródło: Kopalnia Wiedzy