

Stingray – służby dopadną cię wszędzie!

27 czerwca 2018

Na służby specjalne rządy wydają ogromne pieniądze. Nie po to aby chronić obywatela ale po to aby chronić siebie przed nami, wtedy gdy się zorientujemy jak nas robią „w konia”.

Stingray to ryba ze śmiertcionośnym kolcem, którym zabiła jednego ze znakomitych światowych przyrodników. Stingray to jest też urządzenie jakie policja – i nie tylko policja używa – aby z jego pomocą wyśledzić gdzie jesteś, odczytać twoje SMS-y, e-maile, rozmowy...

Służby policji w USA i, jak się wydaje, również w Europie, w tym w Polsce, używają skrycie urządzenie, które znane jest jako Stingray, a służy do monitorowania aktywności telefonu i w ten sposób do śledzenia. Urządzenie jest tak tajne (i faktycznie bezprawne) że ich użytkownikom nie wolno jest powiedzieć nic na temat technologii lub zasady działania – informuje The New York Times.

Zastosowana w nich technologia umożliwia przechwytywanie SMS, e-maili, rozmów telefonicznych i danych dotyczących lokalizacji. Raport „The Times” mówi, że Stingray często uzyskuje informacje na temat urządzeń w pobliżu śledzonego celu, a nie tylko z urządzenia na które jest skierowane.

Urządzenie wywołało kontrowersje w słynnej Dolinie Krzemowej gdy niedawno szeryf powiatu Santa Clara County, Laurie Smith, poprosiła urzędników powiatu by zapłacili 502 000 USD za zakup tej technologii. Pani szeryf odmówiła jednak podania szczegółów na temat działania systemu, poza stwierdzeniem, że wykorzystuje się je do śledzenia telefonów komórkowych, terrorystów i innych przestępców.

Choć nie wiemy zbyt wiele o systemie Stingray, który czasami

idzie nazwany jest KingFish, dziennikarzom udało się zebrać kilka informacji na temat jak jest używany i gdzie.

Co wiadomo o Stingray na podstawie sprawozdań?

Jest w stanie uzyskać dostęp do urządzeń mobilnych, ponieważ wobec telefonu pozoruje że jest wieżą telefonii komórkowej, co często określane jest jako „symulator sieci komórkowej” (symulator stacji bazowej, BTS – przypis).

„Washington Post” opracował graficzny schemat pokazujący jak to działa. Po włączeniu aparatu Stingray, sygnały z pobliskich telefonów są przekierowywane do niego, tak jakby to była wieża komórkowa. Zaprojektowano go tak, że ani sieć serwisu telefonu komórkowego ani użytkownik nie mogą wykryć jego wykorzystania (urządzenie Stingray po prostu udaje, że jest stacją bazową, wysyłając odpowiednie sygnały do telefonów komórkowych. Ma dostęp do danych pochodzących nie tylko od podejrzanego i śledzonego delikwenta, ale również od wszystkich osób, jakie przypadkowo znajdują się w pobliżu – przypis).

Nie można dokładnie ustalić jak powszechnie technologia jest stosowana, ponieważ służby policji (pod nadzorem FBI) są zmuszone do podpisania umów o nieujawnianiu informacji na ten temat. Wygląda jednak na to, że w USA jest w użyciu na terenie całego kraju. Zarówno władze jak i policja posługują się Stingray w Nowym Jorku, na Florydzie, w Teksasie, Wisconsin, Minnesocie i Illinois. Lokalna policja posługuje się tą technologią w Virginii, North Carolinie, Georgii, Missouri, Michigan, Arizonie, Kalifornii, Idaho, Waszyngtonie i na Alasce. Aktywność stosowania Stingray w większości stanów jest nieznana.

Urządzenia są zwykle opłacane przez poszczególne instytucje, a w niektórych przypadkach za symulatory stacji bazowych telefonii komórkowej płaci rząd federalny poprzez dotacje Homeland Security. Choć o Stingray teraz jeszcze nie wiadomo zbyt wiele, urządzenie nie jest nowe. Stróże prawa w Północnej

Karolinie powiedzieli, że używali go już w 2013 r.

Firma Harris, która produkuje urządzenia Stingray, zarobiła już 40 milionów dolarów za swe systemy technologii śledzenia, sprzedając je miastom, stanom i władzom federalnym. Było wiele spekulacji na temat tego, jak informacje uzyskane przez urządzenia StingRay są używane. „W interesie użytkowników jest utrzymanie pełnej tajemnicy, gdyż w grę wchodzi problem ochrony prywatności” – mówi Orin Kerr, ekspert prawa dotyczącego ochrony prywatności z George Washington University. „Cóż jest tak tajemniczego, że próbują to ukryć?” – pyta.

No, ale skoro sprawa zaczęła oglądać światło dzienne, to wcześniej czy później pojawi się coraz więcej konkretnych wiadomości. „W 2008 r. za IMSI Catcher produkcji amerykańskiej trzeba było zapłacić około 170 tys. dolarów, co sprawiało, że był to sprzęt, w który zaopatrywały się głównie służby specjalne. Jednak już w 2010 r. na Defcon (doroczne spotkanie hakerów i specjalistów IT odbywające się w Las Vegas), grupa zapaleńców udowodniła, że urządzenia o podobnych możliwościach zbudować można za 1500 dolarów z możliwych samodzielnie do zdobycia części. Obecnie chiński producent oferuje IMSI Catcher w Internecie w cenie 1800 dolarów za sztukę, co sprawia, że taki sprzęt stał się ogólnie dostępny.”

Autorstwo: Nathanel

Na podstawie: „The Washington Post”

Źródło: NEon24.pl