NSA zainfekowało ponad 50 000 komputerów na świecie

7 maja 2018

Specjaliści zajmujący się bezpieczeństwem cybernetycznym Węgier odkryli a następnie ujawnili kilka brudnych sekretów Agencji Bezpieczeństwa Narodowego (NSA). Zespół utrzymuje, że NSA ma możliwość skanowania i wykrywania grup hakerskich na poziomie krajowym i może łatwo włamywać się do sieci innych narodów, informuje „Wired". Odkrycie dokonano w Laboratorium Kryptografii i Bezpieczeństwa Systemu CrySys.

„W momencie, gdy NSA włamuje się do maszyn w Iranie, Rosji, Chinach czy jeszcze innych krajach, operatorzy Agencji Bezpieczeństwa Narodowego chcą przede wszystkim dotrzeć, do list aktywnych zagranicznych szpiegów z danego kraju. Jest to przedłużenie zimnej wojny, ale na nowym, bardziej zaawansowanym poziomie. NSA zdobywa informacje a następnie przekazuje zdobyte informacje CIA, która przystępuje do werbowania zagranicznych szpiegów, namawia ich do współpracy. W przypadku odmowy niektórzy zostają usunięci" – informuje „Hacker News".

Co więcej, CrySys dotarło do informacji mówiących ich NSA w ciągu zaledwie kilku tygodni było w stanie zidentyfikować ponad czterdzieści różnych operacji międzynarodowych, do których dostęp był ograniczony i stanowił element bezpieczeństwa narodowego poszczególnych krajów. Specjaliści od cyber bezpieczeństwa uważają, że za nielegalne działania NSA jest odpowiedzialna specjalistyczna jednostka wewnątrz agencji zwana „Sporem terytorialnym" lub „TeDi".

Początkowo głównym zadaniem jednostki była identyfikacja i zwalczanie nadchodzących cybernetycznych zagrożeń prowadzonych przeciwko USA lub systemom Agencji Bezpieczeństwa Narodowego. Jednak z czasem programy zostały również wykorzystane do

przeprowadzania ataków na inne państwa. TeDi rozpoczęła działalność, przed którą miała chronić USA.

„Skrypty jednostki NSA używają podpisów cyfrowych do wykrywania APT. Takie sygnatury działają jak odciski palców dla grup hakerskich, mogą zawierać nazwy plików lub fragmenty kodu ze znanego szkodliwego oprogramowania, które zaawansowani hakerzy używają wielokrotnie lub konkretne zmiany, w podstawowych ustawieniach systemu operacyjnego komputera. NSA przejmuje informacje, skrypty i oprogramowanie a następnie używa go przeciwko społeczeństwu. O tym się nie mówi jednak inwigilacja trwa i ma się coraz lepiej" – pisze „Intercept".

To jednak nie wszystko. 6 czerwca 2013 roku, brytyjski „The Guardian" oraz amerykański „The Washington Post" opublikowały obszerne materiały, w których ujawniły dowody potwierdzające szokującą postawę największych przedsiębiorstw branży internetowej. Microsoft, Yahoo INC, Google, Facebook, You Tube, Skype, czy AOL przystąpiły do tajnego programu szpiegowskiego NSA noszącego nazwę PRISM. Innymi słowy Centralna Agencja Wywiadowcza Stanów Zjednoczonych bez żadnego problemu mogła gromadzić informacje o zwykłych obywatelach. Wymieńmy również program o kryptonimie Xkeyscore, którego zadaniem była pełna inwigilacja wszystkich internatów.

„The Guardian" donosi, że pod lupę byli brani także użytkownicy z po za Stanów Zjednoczonych. Z resztą w mediach zrobiło się o tym głośno, kiedy na jaw wyszły informacje, że NSA podsłuchiwała także czołowych polityków UE w tym Kanclerz Niemiec Angelę Merkel. Nie dajmy się zwieść ten, kto polecił stworzenie tych projektów i objęcie nimi czołowych polityków nie działał dla dobra USA, lecz dla dobra interesów pewnych elit, ponieważ informacja jest czymś bezcennym.

Dodatkowo ujawnione zostały takie projekty jak „Tempora" czy proceder oznaczania nowo wyprodukowanych smartfonów. Ujawnione zostały również informacje na temat tak zwanych implantów, czyli programów, którymi NSA zainfekowało ponad 50 000

komputerów na całym świecie. Oprogramowanie to jest nieaktywne i uśpione, lecz może być w konkretnym momencie uaktywnione, jeżeli zaistnieje taka potrzeba.

Autorstwo: Zespół „Globalnego Archiwum”
Źródło: Globalne-Archiwum.pl