Jedna z największych operacji szpiegowskich w internecie

21 lutego 2015
Podobny do Stuxnet wirus zainfekował ogromną ilość komputerów w blisko 42 krajach – informuje Kaspersky Labs.

Od 2001 roku grupa hackerów zainfekowała komputery w co najmniej 42 państwach (patrz mapa wyżej) – ujawnili pracownicy Kaspersky Labs. Redakcja serwisu Ars Technica określiła całą operację jako wymagającą „nadludzkich umiejętności technicznych" sugerujących „nadzwyczajne zdolności i nieograniczone środki". Najbardziej imponującym jest przede wszystkim stworzenie ukrytego obszaru na powierzchni dysku, który pozostawał niewykrywalny dla nawet najbardziej zaawansowanych programów antywirusowych, był także odporny na formatowanie. Dyski twarde pozostają jednym z głównych obszarów sprawdzanych przez specjalistów od bezpieczeństwa, gdyż to właśnie stamtąd najczęściej instaluje się niebezpieczny wirus.

Co budzi największe zaskoczenie to sposób w jaki oprogramowanie trafiało na twarde dyski – znajdowało się ono już w momencie zakupu u producenta. Podejrzewa się, że nie ominęło to wiodących producentów dysków, w tym

Western Digital Corp, Seagate Technology Plc, Toshiba Corp, IBM, Micron Technology Inc and Samsung Electronics Co Ltd, co oznaczałoby, że praktycznie większość rynku została skutecznie zinflitrowana.

Grupa, którą pracownicy Kasperskiego nazwali „Equation Group" oprócz dysków używała także innych środków do rozprzestrzeniania wirusa – korzystano między innymi z dysków USB oraz z płyt CD. Analitycy wskazują, że wirus nazwany przez nich Fanny bardzo przypomina inne złośliwe oprogramowanie – Stuxnet. Zdaniem ekspertów możliwym jest, że to właśnie Fanny

służyła jako aplikacja mająca wybrać główne cele dla Stuxnetu w Iranie a następnie rozprzestrzenić zasięg wirusa.

Skoro więc „Equation Group” udało się przeprowadzić operację wymagającą „nieograniczonych zasobów” to kto ich wspierał? Podejrzenia kierowane są od razu w kierunku NSA, której udowodniono opracowanie Stuxnetu. Podejrzenia te potwierdzają byli pracownicy agencji, którzy w wypowiedzi dla agencji Reutera przyznają, że NSA bardzo ceniła to oprogramowanie, jednak nie są w stanie określić do czego było ono używane.

Autorstwo: Victor Orwellsky
Źródło: Kod Władzy