Cyberszpieg Flame otrzymał rozkaz autodestrukcji

14 czerwca 2012

Cyberszpiegowskie narzędzie Flame zaczyna wycofywać się z zarażonych komputerów i to w taki sposób, aby utrudnione było badanie jego powiązań z twórcami. Można pokusić się o teorię, że osoby stojące za wcześniejszymi narzędziami cyberwojny czegoś się nauczyły.

Pod koniec maja wyszło na jaw, że komputery na Bliskim Wschodzie zostały zaatakowane przez wysoce zaawansowanego szkodnika Flame, który mógł wykradać z nich różnego rodzaju informacje, od dokumentów począwszy na nagraniach rozmów skończywszy.

Flame'a połączono z innymi zaawansowanymi narzędziami, takimi jak Stuxnet i Duqu. Na początku czerwca New York Times ujawnił, że Stuxnet mógł być narzędziem stworzonym przez USA i Izrael w celu zakłócania irańskiego programu nuklearnego. To narzędzie niechcący wymknęło się na wolność. Czy Flame też miał działać tylko w ukryciu na zlecenie jakiegoś rządu?

Wygląda na to, że ujawnienie Flame'a nie było na rękę jego twórcom. Gdy firma Kaspersky Lab jako pierwsza opublikowała informacje o tym cyberszpiegu, zauważono, iż jest on wyposażony w moduł autodestrukcji. W ubiegłym tygodniu firma Symantec odnotowała natomiast, że serwery kontroli Flame'a wysłały do niektórych zainfekowanych komputerów komendę inicjującą samozniszczenie.

Flame „deinstaluje" się w taki sposób, aby nie pozwolić na późniejszą analizę jego aktywności oraz powiązań z twórcami. Specjalny plik browse32.ocx zawiera listę plików i folderów używanych przez Flame'a, które w momencie samozniszczenia są nie tylko usuwane, ale również nadpisywane losowymi znakami. Również moduł odpowiedzialny za autodestrukcję zostaje

ostatecznie usunięty. Badacze Symanteca zaobserwowali ten proces na zainfekowanych komputerach, które zachowano dla celów badawczych.

Komenda autodestrukcji została wysłana do zarażonych komputerów krótko po opublikowaniu informacji na temat Flame'a. Co ciekawe, szkodnik był wyposażony w inny komponent autodestrukcji o nazwie SUICIDE, ale z jakiegoś powodu jego twórcy nie użyli go, decydując się na skorzystanie z browse32.ocx. Trudno powiedzieć dlaczego.

W kontekście wcześniejszych informacji o pochodzeniu Stuxneta można wyciągnąć jeden wniosek – jeśli Stuxnet naprawdę nie miał wyjść na wolność, to tworząc kolejne cyberbronie jego twórcy mogli przewidzieć konieczność autodestrukcji i wprowadzili ją do kolejnych narzędzi. Ktokolwiek robi te szkodniki, bardzo nie chce, by je z nim łączono.

Opracowanie: Marcin Maj
Na podstawie: Symantec
Źródło: Dziennik Internautów