Nowa broń USA?

19 września 2012

Waszyngton może mieć swój udział w stworzeniu wirusów internetowych do szpiegowania i prowadzenia wojny cybernetycznej. Takie są wyniki badania, które przygotowały kompanie IT Rosji i Stanów Zjednoczonych. Nowe wirusy są podobne do tych, które zostały wykorzystane podczas ataku na komputery irańskich obiektów jądrowych. Według danych specjalistów, wiele irańskich komputerów zostało już zarażonych nowym wirusem. Zaatakowane zostały także komputery w Libanie.

W badaniu jest mowa o nowym wirusie podobnym do Flame i Stuxnet. Ten ostatni był wykorzystany do zebrania informacji o irańskim programie atomowym w 2010 roku.

Z pomocą programu Flame mogły zostać skradzione przemysłowe schematy z komputerów w Iranie i Syrii. Wirus został zablokowany. Jednak w tej chwili mowa o nowym niebezpieczeństwie. W każdym razie aktywne są już trzy modyfikacje tych wirusów. I już znane są przypadki zarażenia, co potwierdziło dla „Głosu Rosji" Laboratorium Kaspersky. Skala epidemii może być bezprecedensowa.

Opracowanie takiego stopnia nie mogło zostać dokonane przez prywatne kompanie, mówi Witalij Kamliuk. „Główną cechą wirusa Flame jest to, że w jego opracowaniu brały udział bardzo poważne organizacje. Prawdopodobnie, kontynuują one obsługę programową tego wirusa."

Źródła w rządzie Stanów Zjednoczonych już wcześniej informowały o udziale Waszyngtonu w stworzeniu wirusa Stuxnet. Amerykańskie media informują także, że w stworzeniu cyberwirusa miały swój udział także służby specjalne Izraela. Później zostało ustalone, że Flame i Stuxnet mają podobne kody. Przedstawiciele Laboratorium Kaspersky powstrzymują się

od oskarżeń pod czyimkolwiek adresem. Jednak podkreślają oni, że wraz ze startem Flame i Stuxnet, można mówić o początku nowego etapu w rozwoju cyberbroni.

„Wirus komputerowy po raz pierwszy przekroczył granicę świata wirtualnego i zaczął współdziałać z jego innymi obiektami. Wirus Stuxnet mógł zniszczyć infrastrukturę materialną. Jesteśmy poważnie zaniepokojeni tym, że podobne ataki stają się normą. Opracowanie programów komputerowych kosztuje poważne organizacje mniej niż przeprowadzenie realnej operacji. Program komputerowy jest o wiele łatwiej opracować, obsługiwać i zmieniać. Ponadto, internet w chwili obecnej pozwala na dokonywanie tego typu ataków zupełnie anonimowo.”

Jako najbardziej niebezpieczna cechę cyberbroni specjaliści podają szybkość jej działania. Atak, na przykład na obiekt atomowy w Iranie czy inny rządowy obiekt w jakimś państwie, odbywa się natychmiastowo. Znika konieczność wykorzystania zasobów ludzkich.

Źródło: Głos Rosji