

Спецслужбы США и Израиля создали вирус для похищения секретной информации, последующих кибератак и саботажа.

Продвинутый компьютерный вирус под названием Flame, который собирал разведданные и готовился для проведения кибератак, направленных на замедление кампании Ирана по созданию собственного ядерного оружия, совместно разработан по заказу властей США и Израиля, сообщает CNews со ссылкой на Washington Post и анонимные источники среди западных чиновников, осведомленных об этой инициативе США и Израиля.

О программе Flame эксперты российской «Лаборатории Касперского» говорят, как о «возможно, самом сложном вирусе в истории», а в прессе называют «самым опасным кибероружием», собирала данные о местоположении иранских правительственных компьютерных сетей, а также занималась мониторингом активности в них, отсылая своим создателям массивные потоки секретных материалов в рамках подготовки к масштабным кибератакам против Ирана.

Как пишет Washington Post, в данной инициативе активно участвовали Агентство Национальной безопасности США, ЦРУ и израильские военные, а при создании Flame специалисты этих организаций использовали образцы различных опасных деструктивных программ, таких как вирус Stuxnet, которые должны были вызывать различные неполадки в иранском оборудовании, использовавшемся для обогащения урана.

Аналитики отмечают, что новая информация о вирусе Flame раскрывает дополнительные детали о первой в истории масштабной кампании правительства США по проведению кибератак на правительственном уровне и саботажа через компьютерные сети.

«Речь идет о подготовке поля боя для тайных операций другого типа. Вирусы Flame и Stuxnet являются одними элементами более масштабной атаки, которая все еще продолжается сегодня. Похищение секретной информации у Ирана с помощью вируса является очередным, но не последним шагом в этом направлении», - заявил один из бывших высокопоставленных сотрудников американской разведки на условиях анонимности.

Вирус Flame был обнаружен экспертами «Лаборатории Касперского» в мае 2012 г. в ходе расследования, инициированного «Международным Союзом Электросвязи» (ITU).

Программа-шпион была найдена в ряде стран, преимущественно относящихся к ближневосточному региону. После своего внедрения в систему, Flame способен проводить комплекс действий, например, перехват сетевого трафика, снятие скриншотов, запись аудио-разговоров, перехват клавиатуры, и т.п. Все похищенные данные доступны для операторов трояна через командные серверы.