Год назад программа-"червь" Stuxnet произвела в мире фурор как первое компьютерное супероружие, существование которого подтверждено официально, пишет The Christian Science Monitor. Гамбургский эксперт Ральф Лангнер расшифровал код "заряда" Stuxnet и объявил, что это военное кибероружие, нацеленное на ядерные объекты Ирана, напоминает журналист Марк Клейтон.

Вскоре Лангнер и его коллеги сообщили, что "червь" стремился поразить центрифуги, на которых обогащается уран. По словам Лангнера, Stuxnet разгонял моторы центрифуг и оборудование буквально разлеталось на куски. "При этом Stuxnet создавал иллюзию случайных поломок, чтобы операторы не догадались, что всему виной коварное кибероружие", - говорится в статье.

Но применение Stuxnet может стать пирровой победой для его создателей, полагает издание. А создала червя некая держава с изощренным кибероружием - возможно, США или Израиль, по предположениям Лангнера. "Подобно бомбардировке Хиросимы, Stuxnet впервые продемонстрировал зловещие возможности: в данном случае хакерам, шайками киберпреступников и странам, которые только обзаводятся кибероружием", - пересказывает газета интервью Лангнера.

Скачав Stuxnet из интернета в качестве "чертежа", любой тупоголовый хакер может научиться конструировать и продавать кибероружие "хакерам-активистам" и террористам, которые хотят отключить электричество в целом городе или выпустить облако ядовитых газов, говорит Лангнер.

Эксперт неутешительно оценил ситуацию с кибербезопасностью в Америке. В прошлом году специалисты порекомендовали всем владельцам электростанций, химических заводов и прочих объектов США уделить защите компьютерных сетей приоритетное значение. "Этих тревожных звоночков хватило только на неделю. Затем все вновь впали в кому", - утверждает Лангнер. По его словам, конкретных мер не порекомендовали даже министерство национальной безопасности США и компания Siemens, чью систему атаковал Stuxnet.

Тот факт, что министерство и владельцы объектов не осознали угрозу хакерских атак, копирующих Stuxnet, Лангнер считает самым опасным явлением за истекший период. "Все бреши, которые эксплуатировались, никуда не делись. Всем все равно", - сокрушается он.

"Боюсь, контроль кибервооружений невозможен", - продолжает Лангнер, поясняя, что написание и распространение программ по интернету предотвратить невозможно. Поэтому первоочередная задача - создать оборону компьютерных систем в сферах энергетики, водопровода и химической промышленности. Это дорого, но несоизмеримо с ущербом от хакерских атак.

Если раньше максимум пять человек могли применять "червей" типа Stuxnet, то сегодня таких людей уже более 500, полагает Лангнер. "Теперь некоторые части Stuxnet можно попросту скопировать", - поясняет он. На базе этих частей может быть создана "простая, но эффективная виртуальная "грязная бомба", - предостерег Лангнер. Гением для этого быть не требуется.

"Почему вы сами недавно продемонстрировали, как легко устроить атаку Stuxnet для отключения промышленной системы?" - спросили журналисты.

"Не мог больше терпеть. Мы потеряли целый год, потому что никто не прислушивается", - ответил Лангнер. "Некоторые ключевые элементы я опустил, чтобы программой нельзя было пользоваться", - добавил он.

По работе Stuxnet можно предвидеть, как будет выглядеть война в будущем, полагает Лангнер. Stuxnet также ставит политические вопросы: "Готовы ли США отключить электросети в другой стране, если это ударит в основном по мирному населению? Могут ли и должны ли вести кибервойну гражданские наемники вместо военных? Что случится, когда торговцы начнут поставлять сверхсовременное кибероружие террористам?". Лангнер опасается, что "червь" открыл ящик Пандоры.

Марк Клейтон
The Christian Science Monitor
InoPressa.ru