К ОРУЖИЮ!

Первый выстрел кибервойны

Николай Федотов, ведущий аналитик InfoWatch

То, о чем так долго говорили айтишники и лгали киношники, свершилось. Вредоносная программа впервые поразила стратегический объект на территории противника. Из истории со Stuxnet уши торчат настолько отчетливо, что у знающих людей нет сомнений: программа писалась под конкретный реактор. Прочие компьютеры, флэшки и другие носители Stuxnet заражал, но вреда не причинял. (Кстати, некоторые наивно полагают, что, отключив локальную сеть от Интернета, они застраховали себя от внешних угроз.) Он имел в своем коде странное условие срабатывания, которое долго не могли понять специалисты-антивирусники. Как позже обнаружилось, условие это выполняется лишь на единственной в мире АСУ единственного атомного реактора.

Для размножения и распространения Stuxnet использовал несколько разных уязвимостей, причем достаточно дорогих. Сведения об уязвимости и соответствующий эксплоит на черном рынке стоят денег. Особенно дорого ценится так называемый «0-day» эксплоит (или «0-day» уязвимость). Это «дырка», о которой еще не знает производитель. Используя ее, вирус имеет временную фору и зеленый свет во всех системах.

Позволить себе использование «0-day» может далеко не каждый вирусописатель. А Stuxnet имел в арсенале сразу несколько таких уязвимостей. Следовательно, эту вредоносную программу заказывал миллионер. Или тот, кто денег не считает, ибо на госбюджете. Зато с таким пробивным арсеналом Stuxnet не мог не добраться до цели.

Как вредоносная программа, Stuxnet достаточно обычный червь-троян. Просто навороченный и живучий. Самое интересное и уникальное в нем — та «боеголовка», которую он несет. Stuxnet поражает только один атомный реактор в мире. Все другие компьютеры и информационные системы от него почти не страдают, он их использует лишь для распространения.

Судя по всему, первый выстрел кибервойны достиг цели. Наверняка какие-нибудь майоры отчитались перед какими-то генералами об успешной операции. Следует ожидать запуска кибероружия в серию.

Итоги

Реальные вирусы на реальных предприятиях

Объект	Инцидент
Блок 2 ядерной станции Hatch (штат Джорджия, США), 7 марта 2008 года	Внештатное аварийное выключение на 48 часов после установки обновления ПО (похожий инцидент случился в 2006 году на ядерной станции Browns Ferry из-за нештатного сбоя программируемого логического контроллера).
Корпорация Tennessee Valley Authority (TVA) (в ведомости данной энергетической корпорации находится 11 угольных станций, 8 ТЭС, 3 ядерные станции, 29 ГЭС США), май 2008 года	Проверка регуляторов (GAO, HHS) выявила порядка 2000 уязвимостей разной степени критичности. Среди брешей в безопасности были выявлены сегменты производственной сети, подключенные к Интернету, уязвимости прикладного ПО, отсутствие обновлений безопасности, ошибки в проектировании архитектуры сети и каналов обмена данными.
Центр полетного планирования Федерального управления гражданской авиации США, 26 августа 2008 года	Диспетчерские трех десятков американских аэропортов выведены из строя в результате компьютерного сбоя в центре полетного планирования.
Сбой движения поездов немецких железных дорог (DB), 14 января 2009 года	Компьютерный сбой привел к приостановке системы бронирования и продажи билетов, диспетчеризация движения поездов осуществлялась ручным способом.
Электроэнергетическая сеть США, апрель 2009 года	Силовыми структурами США зафиксировано проникновение в электроэнергетическую сеть и размещение в ней программных «закладок» с целью нарушения корректной работы функциональных элементов.
Энергетическая компания LCRA (Lower Colorado River Authority), 5 апреля 2010 года	Специалистами LCRA зафиксировано свыше 4800 попыток получения доступа к их компьютерной системе.

ИСТОЧНИК: ВИРУСЛОКАДА, 2010 Г.