# Информатизация общества – новые цели для кибероружия

**Денис Гасилин,** *руководитель отдела маркетинга SafenSoft*

Слово "кибервойна" в сознании обычного человека обросло множеством мифов. Существует два весьма распространенных мнения о том, как выглядит стандартная кибератака. С одной стороны, большинство людей ассоциируют со словом "кибервойна" единичные инциденты[1] и не считают информационные угрозы действительно критичными для стран и организаций, сферой деятельности которых не является Интернет или ПДн. С другой – массовая культура представляет кибератаки некой всемогущей силой, применением сверхсовременных видов оружия, полностью уничтожающего или берущего под контроль неудачливую жертву[2].

Любители громких терминов спешат навесить ярлык "кибервойна" на любое действие вплоть до взлома Web-сайта с изменением заглавной страницы.

## Истина – посередине

Кибервойна возможна лишь в весьма ограниченном пространстве и против определенных целей, но последствия могут быть крайне разрушительными.

Первым общеизвестным вредоносным кодом, использовавшимся как кибероружие, стал червь Stuxnet. Созданный примерно в 2005 г., а обнаруженный в 2010 г. благодаря счастливой случайности: компьютер иранского клиента белорусской фирмы "ВирусБлокАда" впал в цикл перезагрузок в результате нештатной работы вредоносного кода, созданного для незаметного перевода производственных механизмов за пределы безопасных параметров. Обнаруженная в коде уязвимость нулевого дня заинтересовала экспертов ИБ, и вирус был не только добавлен в антивирусные базы, но и досконально изучен. Обнаруженная в 2013 г. экспертами Symantec версия 0.5 вредоносного кода позволила детально изучить эволюцию кода. Червь был запрограммирован на распространение через USB, что позволяло вторгаться в защищенные от воздействия из мировой сети объекты. Также он имел подробный алгоритм создания и загрузки своих модулей в атакуемую систему в зависимости от работы на компьютере определенных защитных решений. Таким образом Stuxnet старался свести к минимуму воздействие на заведомо защищенную достаточным образом систему во избежание обнаружения. Одним из 11 решений, которых опасаются разработчики кибероружия, оказалось наше.

Уже больше года продолжаются DDoS-атаки группы кибервоинов Изза ад-Дина аль-Кассама (Izz ad-Din al-Qassam Cyber Fighters) на североамериканские банки. По расчетам активистов, каждая минута успешной атаки против выбранных ими целей стоит жертве $30 000. Некоторые эксперты считают эти атаки местью Ирана за кибератаку против атомных объектов. По их расчетам, этот киберконфликт будет только разрастаться, и уже сейчас, помимо непосредственных атак по отказу от обслуживания, банки ощущают на себе новые методы взлома учетных записей сотрудников и системных администраторов, приводящие к существенным финансовым потерям.

## Потенциальные цели

Информатизация общества постоянно создает новые потенциальные цели для кибероружия. Любое медицинское учреждение с тяжелым оборудованием вроде томографов способно стать жертвой специально разработанного вредоносного кода, отдельные электростанции и даже системы ПВО могут быть выведены из строя по невнимательности или злому умыслу. Разумеется, подобные объекты становятся целью кибератаки в случае полномасштабной войны или террористического акта, но кибервойна может быть и экономической.

Например, добыча сланцевого газа. ПО, необходимое для использования этого метода добычи полезных ископаемых, крайне сложно в эксплуатации и непосредственно управляет оборудованием, ответственным за глубинные гидроразрывы пласта. Любое нарушение в работе этого ПО грозит серьезными последствиями[3]. Перспективы для кибервойны в этой области огромны, и никто не может гарантировать, что они уже не идут и что первые образцы вредоносного кода, направленного против бурильного оборудования, не будут обнаружены через пять лет после создания.

Из этого следует вывод – для защиты от кибероружия, направленного на определенную цель и созданного с использованием уязвимостей нулевого дня, недостаточно использовать традиционные решения, основанные на сканировании сигнатур. Обнаружение такого вредоносного кода – дело случая, даже если оно и произойдет, ущерб к этому времени уже будет нанесен.

## Пути решения

Необходимо применять новые технологии защиты информации, основанные на предотвращении изменений в системе в принципе, вне зависимости от способности идентифицировать вредоносный код во время сканирования. Для критически важных объектов правильным подходом будет создание заведомо безопасного образа системы и дальнейшее предотвращение любых несанкционированных модификаций в файловой системе, реестре или отдельных файлах. Даже динамическая библиотека может стать дверью в систему для злоумышленника, атакующего систему созданным специально под нее вредоносным кодом, использующим уязвимости нулевого дня. Только технологии проактивной защиты способны защитить компьютер в любых условиях и от любых угроз, будь то рабочее место сотрудника, сервер с базой данных или АСУ ТП.

[1] Например, червь Stuxnet, который использовался против иранских центрифуг по обогащению урана, или прошлогодняя DDoS-атака на южнокорейские банки.

[2] Такое представление, разумеется, неверно, так же как был неверен существовавший еще 10 лет назад в массовом сознании образ хакера как всемогущего одиночки.

[3] По неподтвержденным данным, землетрясения в Ланкашире, Англия, причиной которых стало пробное бурение в Блэкпуле, были вызваны некорректной работой ПО, контролирующего оборудование для бурения. Неудачно сработавшая после копирования информации DRM-система оказалась достаточной причиной для приостановки разработок месторождения на два года и возникновения протестных движений в регионе.

NM
АДРЕСА И ТЕЛЕФОНЫ компании SAFENSOFT см. стр. 56