ВОЙНА ИДЕТ ПО ПРОВОДАМ

В XXI ВЕКЕ ВОЕННЫЕ ДЕЙСТВИЯ ЛИШЬ ОТЧАСТИ ПРОИСХОДЯТ В ФИЗИЧЕСКОМ МИРЕ — БОЛЬШИНСТВО ОПЕРАЦИЙ ПРОВОДИТСЯ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ. ЕСТЬ ПРОГНОЗЫ О ТОМ, ЧТО УЖЕ В БЛИЖАЙШИЕ ГОДЫ ВОЙНА КАК ЯВЛЕНИЕ ПОЛНОСТЬЮ ПЕРЕМЕСТИТСЯ В СФЕРУ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ОКОНЧАТЕЛЬНО ПРИОБРЕТЕТ ВИД КИБЕРВОЙНЫ. СВЕТЛАНА РАГИМОВА

EPA / ТАСС

ПЕРВЫЙ ОБРАЗЕЦ КИБЕРОРУЖИЯ В ИСТОРИИ ЧЕЛОВЕЧЕСТВА — ЧЕРВЬ STUXNET, ПОЯВИЛСЯ ВСЕГО ПЯТЬ ЛЕТ НАЗАД

Беспилотные автомобили и самолеты, интернет вещей, «умная» инфраструктура, подключенные ЛЭП, канализации и водоснабжение, светофоры и холодильники. Звучит как рассказ о прекрасном светлом будущем. Но не стоит смотреть на эти явления сквозь розовые очки. На одной из конференций Иван Новиков, основатель компании Wallarm, защищающей веб-ресурсы от хакерских атак, прямо во время своего выступления взломал чайник, демонстрируя, что уязвимым может стать любой предмет — достаточно лишь подключить его к интернету. Вместо нагревательного прибора бытового назначения «плохие парни» так же легко могут добраться и до оборудования электростанции, использующей технологии Smart Grids. А если удастся взломать атомный генератор или атаковать системы управления нефтяными вышками, то и ядерного оружия не надо.

Три года назад в Иране и на Ближнем Востоке эксперты «Лаборатории Касперского» обнаружили признаки кибервойны, проанализировав код вируса Flame. Этот червь был создан для кибершпионажа, и, как сообщили представители компании, над ним поработала группа профессионалов, создавшая один из самых совершенных на тот момент образцов кибероружия. Flame удалял конфиденциальные данные с компьютеров, расположенных в целевых странах, анализировал сетевой трафик, делал скриншоты, записывал разговоры, перехватывал нажатия на клавиатуре и т. д. Все эти сведения вирус передавал операторам через командные серверы. При необходимости Flame могла запустить один или несколько из двух десятков специальных модулей разного назначения. Предшественник этого червя, атаковавший компьютеры Израиля и США в 2010 году, содержал гораздо менее изощренный программный код.

Гонка вооружений в киберпространстве началась и развивается не менее быстро, чем «мирные» технологии. Первый образец кибероружия в истории человечества — червь Stuxnet, появился всего пять лет назад и смог отключить 900 центрифуг иранского завода по обогащению урана. Хосе Игнасио Торребланка, глава мадридского офиса Совета Европы по иностранным делам, профессор политических наук Национального университета дистанционного образования Мадрида, объясняет, что сегодня гораздо легче атаковать нефтяные вышки страны цифровым путем, чем физическим. «Сегодня цифровые уязвимости быстро становятся главной заботой правительства и бизнеса. По последним оценкам, только 11% компаний нефтяной отрасли сообщают, что чувствуют себя защищенными от подобных атак, и, что еще хуже, 23% признаются в том, что не используют в своих сетях средства мониторинга для обнаружения попыток нападений»,— говорит Хосе Торребланка.

Финское правительство в 2013 году обнаружило шпионскую программу неизвестного происхождения, которая в течение многих лет работала на компьютерах чиновников. В США в ноябре прошлого года вирус, чье авторство приписали Китаю, заразил метеорологические спутники, чтобы обнаружить уязвимости в сети, обслуживающей систему глобального позиционирования GPS, играющую существенную роль в обороноспособности страны. Простая USB-флешка может быть более вредоносной, чем бомба с лазерным наведением; нефтяной поток можно прервать с помощью компьютера; военные спутники можно просто отключить вместо того, чтобы разрушать их. Очевидно, мы являемся свидетелями революции в военном деле. XX век был веком физики, и в это время велись физические войны, XXI век — цифровой, и можно ожидать, что войны также будут цифровыми. И здесь большой вопрос — физическая смерть противника также будет считаться чем-то устаревшим или все еще останется необходимым условием для победы.

ГЛОБАЛЬНАЯ СЛЕЖКА В ИНТЕРНЕТЕ, КОТОРУЮ ОСУЩЕСТВЛЯЕТ АГЕНТСТВО НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ США (АНБ),— ЭТО ЛИШЬ ЧАСТЬ СУЩЕСТВУЮЩЕЙ АМЕРИКАНСКОЙ КИБЕРСТРАТЕГИИ

ФИСТАШКОВЫЙ ЗАПАХ Как правило, проследить стартовую точку, с которой началось распространение вируса, подобного Flame или тому, что действовал в финском правительстве, почти невозможно. Как и доказать, что программу разработали кибервойска какой-либо страны. Составителям отчета о растущей киберугрозе со стороны Ирана под названием «Урожай фисташек» (Pistachio Harvest Project) это удалось. Результаты совместного исследования, проведенного Norse Corporation и командой Critical Threats Project из American Enterprise Institute, были опубликованы в апреле. Исследователи собирали данные о действия киберармии Ирана, распространив по всему миру несколько миллионов «сенсоров» — фальшивых веб-сайтов с уязвимостями, которые «прикидываются» обычными сайтами банков, университетов, заводов, электростанций и прочих объектов, которые могут быть интересны хакерам. В результате анализа собранных данных выяснилось, что злоумышленники пытаются обнаружить и взять под контроль слабозащищенные системы SCADA (автоматизированные системы диспетчерского управления и сбора данных) — например, те, что обслуживают электроэнергетическую инфраструктуру. При этом зловредное ПО искало уязвимости и, по мнению исследователей, отправляло информацию о них в специальную базу данных.

Кибервойска и группы, разрабатывающие кибервооружение, создаются в рамках специальных программ в США и в других западных странах. Кибероборона в соответствии с подходом, которому следует НАТО, это возможность использования информационных сетей для того, чтобы парализовать органы управления и систему обороны той или иной страны, а после этой информационной атаки уже приступить непосредственно к военному воздействию.

Уже в 2010 году США создали собственное кибернетическое командование. Американские власти уверяют, что оно занимается исключительно обороной сетей. В том же году, как было установлено экспертами, спецслужбы США провели атаки на иранские ядерные объекты, чтобы вывести их из строя.

Как следует из новых рассекреченных Эдвардом Сноуденом материалов, опубликованных изданием Der Spiegel, США готовятся к кибервойнам за господство в интернете. Доказательством этому являются документы о находившемся в ведении американских спецслужб проекте Politerain. В рамках данного проекта осуществлялся набор и обучение специалистов, способных путем внедрения вредоносного ПО выводить из строя компьютерные системы, контролирующие работу объектов инфраструктуры и телекоммуникации потенциального противника, а также перехватывать его денежные трансакции. Сверхзадачей проекта было воспитать у будущих сотрудников спецслужбы «мышление атакующего».

Глобальная слежка в интернете, которую осуществляет Агентство национальной безопасности США (АНБ),— это лишь часть существующей американской киберстратегии. С военной точки зрения это «Фаза 0» в стратегии кибервойны, к которой готовятся США. Как следует из рассекреченных документов АНБ, цель этой слежки — нащупать слабые звенья в системах противника. Внедрение шпионского ПО (киберагентурная сеть) и получение