Кибервойна: день первый

Андрей МАСАЛОВИЧ,
руководитель направления конкурентной разведки, АО «ДиалогНаука»

Представим себе гипотетическую картину: мы проснулись, а за окном – кибервойна. Что мы увидим? Перегруженные перекрестки, многокилометровые пробки и транспортный коллапс на улицах (хакеры уже многократно демонстрировали перехват управления светофорами, приводящий к хаосу на дорогах). Подтопленные улицы и следы экологической катастрофы в водоемах (увы, сброс содержимого очистных сооружений в реку и, наоборот, блокировка слива городской канализации также уже продемонстрированы хакерами на практике). Если за окном будет ночь или сумерки, мы вообще не увидим ничего: атаки на энергетическую инфраструктуру давно отработаны и позволяют отключать электричество в целых регионах.

Зато мы увидим отблески пожаров во многих окнах. Сегодня в большинстве домов уже присутствуют бытовые приборы, допускающие управление через Интернет – и это не только смарт-телевизоры или холодильники, но и чайники, утюги и радио-няни. Перехватив управление этими устройствами, хакер с легкостью может перевести их в режим зажигалки.

Удаленные поселки останутся без связи. Низменные районы будут затоплены в результате аварий на плотинах ГЭС. Обширные территории на годы окажутся зараженными вследствие взрывов на энергоблоках АЭС. Ослепнут системы управления воздушным движением, и только чудо спасет находящиеся в воздухе самолеты. Отключатся все привычные нам каналы связи, и единственным видом информации, доступным населению, окажется вражеская пропаганда – она, наоборот, будет поступать бесперебойно через все окружающие компьютеры и гаджеты. При этом шансы на оперативный адекватный ответ со стороны военных упадут до нуля: оборудование, обеспечивающее решение военно-стратегических задач, будет выведено из строя в первые минуты атаки наряду с другими компонентами критической инфраструктуры страны.

Выглядит как апокалиптический бред? Однако все перечисленные виды атак (и их результаты) уже были продемонстрированы хакерами (и кибервойсками) разных стран, правда, пока по отдельности.

Ежегодно в конце мая в Москве проходит популярная конференция Positive Hack Days, в рамках которой организаторы устраивают конкурс атак на макет города. На большом столе собран макет, в котором есть игрушечные железные дороги, дома, мосты, плотины, электростанции и другие компоненты городской жизни, управляемые фрагментами реальных программ (используемых в настоящих системах управления). Соответственно, если мы видим, как хакер пускает под откос игрушечный поезд – то же самое он с легкостью проделает и с реальным экспрессом. Так вот, в прошлом году старшекласснику удалось разрушить плотину и вызвать затопление, а в этом году хакеры разнесли весь город.

Итак, угроза масштабных кибератак, причем как со стороны киберподразделений различных стран, так и со стороны международных террористических организаций и даже автономных групп хакеров, стала реальной и требует принятия немедленных адекватных мер. Каких?

Во-первых, требуется развертывание глобальной системы контроля оперативной обстановки в киберпространстве и раннего предупреждения о подготовке и осуществлении кибератак. Все ключевые компоненты такой системы уже существуют и опробованы, причем Россия по многим направлениям находится в привилегированном положении: базовые технологии антивирусов (Касперский), интернет-разведки (Avalanche), управление уязвимостями (Max Patrol) и другие имеют отечественное происхождение.

Во-вторых, необходимо комплексное изучение «уязвимостей нулевого дня» – технологической основы для современных троянских программ (как атакующего, так и разведывательного назначения).

Утечки боевых программ АНБ и ЦРУ, опубликованные порталом WikiLeaks с февраля по апрель, содержат более 120 новых эксплойтов, и весь этот арсенал уже попал в руки хакеров.

В-третьих, нужен комплексный подход к созданию систем обеспечения информационной безопасности. Атака вируса-шифровальщика WannaCry 12 мая текущего года показала тотальную неготовность традиционных средств обеспечения информационной безопасности к новым видам атак. К слову сказать, уязвимость MS 017-10, использованная WannaCry, известна профильным специалистам с 2006 г., с момента, когда Microsoft внедрила драйвер SMB v2, но оставила в составе ОС его «дырявого» предшественника – SMB v1. Некоторые исследователи даже предполагают, что это была преднамеренная закладка, и представители «традиционной» ИБ десятилетие не обращали на нее внимания.

Далее, необходимо всемерно развивать технологии интернет-разведки и разведки по открытым источникам (OSINT) для решения практических задач сбора и аналитической обработки оперативно значимой информации в интересах подразделений кибербезопасности различных ведомств. Для этого требуется согласованное решение следующих задач:

- обеспечение скрытности присутствия в Сети и бескомпроматность работы. В арсенале киберподразделений ведущих держав присутствует обширный арсенал приемов – от использования VPN, прокси-серверов и сети TOR до массового заражения маршрутизаторов;
- сбор информации из глубинного («серого») Интернета, а также из социальных сетей. Специализированные инструменты поиска, базирующиеся в облаке, позволяют вести долгосрочное скрытое наблюдение за заданными сетевыми ресурсами, включая аккаунты и группы в социальных сетях, сообщения в мессенджерах и т. д.;
- анализ профилей пользователей в социальных сетях. Детальный поведенческий анализ на основе принципов психометрии (Psyhometrics) позволяет выявлять пользователей с заданными психическими свойствами и отклонениями (склонность к алкоголю и наркотикам, жестокость, суицидальные наклонности, экстремизм и т. д.). Эта информация в последующем используется при формировании контрактных и специальных подразделений, а также в ряде других задач;
- анализ пользовательских групп в социальных сетях. Методы облачной обработки больших данных (включая нейронные сети, нечеткую логику и др.) позволяют выявлять места скопления целевой аудитории для планирования и проведения операций в сфере информационной войны;
- мониторинг Интернета вещей в целях выявления плохо защищенных компонентов инфраструктуры других стран, как военной, так и транспортной, энергетической и др.;
- контроль собственной защищенности. Анализ хакерских атак нового поколения (WannaCry, Petya и др.) показал, что традиционные антивирусы и сканеры не справляются с защитой критических ресурсов, нужны новые комплексные решения;
- раннее обнаружение утечек критической и конфиденциальной информации. Организация облачной системы контроля распространения информации позволяет оперативно обнаруживать утечки важной информации как общегосударственного, так и военного применения.

> Угроза масштабных кибератак, причем как со стороны киберподразделений различных стран, так и со стороны международных террористических организаций и даже автономных групп хакеров, стала реальной и требует принятия немедленных адекватных мер.

> Нужен комплексный подход к созданию систем обеспечения информационной безопасности.

Таким образом, решение перечисленных проблем с успехом может быть использовано для выполнения комплекса оперативно-стратегических задач в киберпространстве в интересах обороны и безопасности. ■