ЛОВЛЯ В МУТНОЙ ВОДЕ

ОКОЛО $1 МЛРД ЕЖЕГОДНО СОСТАВЛЯЕТ УЩЕРБ ОТ КИБЕРПРЕСТУПЛЕНИЙ, КОТОРЫЕ С КАЖДЫМ ГОДОМ СТАНОВЯТСЯ ВСЕ БОЛЕЕ ГРАМОТНЫМИ И ИЗОЩРЕННЫМИ. ГЛАВНЫЕ ПРОБЛЕМЫ В БОРЬБЕ С КОМПЬЮТЕРНЫМИ АТАКАМИ — ЭТО СЛОЖНОСТЬ ПОИСКА ВИРТУАЛЬНЫХ ЗЛОУМЫШЛЕННИКОВ, РАЗОБЩЕННОСТЬ И НЕСОВЕРШЕНСТВО ЗАКОНОДАТЕЛЬСТВА РАЗНЫХ ГОСУДАРСТВ, НИЗКИЙ УРОВЕНЬ ГРАМОТНОСТИ НАСЕЛЕНИЯ В ВОПРОСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ). ВЛАДА ГАСНИКОВА

ЕВГЕНИЙ ПАВЛЕНКО

ГЛАВНАЯ СЛОЖНОСТЬ КИБЕРПРЕСТУПЛЕНИЙ ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО ПРЕСТУПНИК ФИЗИЧЕСКИ МОЖЕТ НАХОДИТЬСЯ В ОДНОЙ ТОЧКЕ ЗЕМНОГО ШАРА, А ЖЕРТВА СОВСЕМ В ДРУГОЙ

Специалисты классифицируют виды киберугроз с помощью условной пирамиды. В ее основании находится так называемая «традиционная» киберпреступность. Ее отличительными чертами является массовость атак и всенаправленность, что больше всего угрожает обычным пользователям. Основной целью злоумышленников является получение прямой финансовой выгоды. Банковские троянцы, спам-боты, троянцы-вымогатели, мобильные угрозы — по оценке «Лаборатории Касперского», на них приходится более 80% от общего количества современных угроз.

Второй уровень — это угрозы для бизнеса: промышленный шпионаж, кража интеллектуальной собственности и целевые хакерские атаки, задача которых дискредитировать жертву. Атакующие узко специализируются либо под конкретную цель, либо под конкретного заказчика

На третьем уровне располагается «кибероружие» — вредоносные программы, создание и финансирование которых осуществляется государственными структурами разных стран мира. «Такое программное обеспечение применяется против граждан, организаций и ведомств других государств. Оно может быть предназначено для уничтожения баз данных и информации в целом, для шпионажа и даже для причинения физического ущерба. На подобные угрозы в общем объеме приходится около 1%, но они самые успешные и противостоять им сложнее всего», — рассказывает управляющий директор «Лаборатории Касперского» в России и странах СНГ Сергей Земков. По его наблюдениям, сложные целевые атаки перестали быть «проклятьем» лишь военных, правительственных, научно-исследовательских и критически важных инфраструктурных организаций: киберпреступники перенимают подобные инструменты для нападения на бизнес, в первую очередь — из финансового сектора.

По оценкам специалистов, рынок киберпреступности в мире может достигать $1 млрд в год. Это примерные цифры, потому что про часть атак аналитики и эксперты могут даже никогда не узнать.

ГЛАВНЫЙ МОТИВ Менеджер по продукту Blindspotter компании Balabit Петер Гъенгеши приводит данные из ежегодного отчета Verizon Data Breach Investigation Report: по данным за 2016 год, самым распространенным мотивом киберпреступлений является финансовая выгода — кража или вымогательство денег у жертвы. Второй по популярности — шпионаж, вместе они составляют свыше 93% от всех совершаемых атак в мире. «Политические мотивы или личные обиды иногда стоят за некоторыми взломами, но они в меньшинстве. Около 25% атак выполняются инсайдерами, остальные 75% приходятся на внешнюю среду. Около половины атак могут быть связаны с преступными группами и около 18% — с госструктурами. Четыре из пяти инцидентов происходят по вине слабого или скомпрометированного пароля, а половина — с использованием какого-либо вредоносного ПО», — говорит господин Гъенгеши.

Результаты кибератак могут иметь разную форму, но всегда денежный урон от них велик. Например, в 2008 году произошла одна из самых известных кибератак на критические инфраструктуры: вирус Stuxnet вывел из строя урановые центрифуги на иранском заводе, остановив тем самым ядерную программу, вспоминает консультант по информационной безопасности «Диджитал Дизайн» Станислав Грибанов. «В конце 2015 года Украина подверглась кибератаке на свою национальную электросеть, в результате чего свыше 200 тыс. жителей (по некоторым оценкам — до 600 тыс.) остались без электричества. Из последних событий — майская международная атака вирусом-вымогателем WanaCrypt0r. Это была самая массовая кибератака с использованием криптотрояна. Им были поражены самые важные общественные структуры почти сотни стран: правительственные учреждения, банки, системы здравоохранения, телекоммуникационные сервисы, транспортные и другие компании», — перечисляет господин Грибанов. Этот вирус поразил более 230 тыс. компьютеров в 150 странах буквально за сутки. Все данные на них были заблокированы, стоимость освобождения одного компьютера составляла €300–600.

Самая крупная разовая киберкража — это $81 млн, которые злоумышленники вывели из ЦБ Бангладеш. Червь Carbanak был нацелен на банки по всему миру, приблизительная сумма от его ущерба оценивается в $1 млрд. В 2014 году случился взлом компании Yahoo, который привел к утечке данных 500 млн пользователей сервиса. Несмотря на масштаб атаки, общественности стало известно о ней только спустя два года.

Кроме того, существуют и неочевидные угрозы: это преступления, совершаемые с использованием компьютеров, мобильных устройств или сетей связи. «Например, конфиденциальные документы могут быть сфотографированы на смартфон и отправлены через мобильный интернет или распечатаны из системы электронного документооборота для продажи или публикации. Такие инциденты могут наносить репутационный ущерб или прямые финансовые потери», — рассказывает генеральный директор компании «ЭвриТег» Антон Самойлов. По его словам, специалисты по информационной безопасности пока редко задумываются о них, хотя таким образом происходит до 20% утечек. «Вероятно, в результате развития и повсеместного использования DLP-систем доля утечек на бумажных носителях будет увеличиваться: поймать сотрудника, выносящего распечатку в сумке, можно только при поголовном досмотре персонала на выходе из офиса — чего, разумеется, почти никто не делает, и отследить такой канал почти невозможно. Защитить информацию в этом случае можно только на стадии печати или отображения на экране, и рынок средств защиты от таких угроз сейчас только формируется», — говорит господин Самойлов.

По оценке ведущего специалиста департамента сетевой безопасности RCNTEC Германа Наместникова, ежедневно в мире совершаются миллионы киберпреступлений, в основном экономического характера. «Большую часть этих атак проводят одиночки или групп злоумышленников, которые не обладают достаточной квалификацией для проведения масштабных атак. Тем не менее они создают определенный информационный шум, в котором легко может затеряться деятельность квалифицированных киберпреступников, и это создает дополнительные сложности при расследовании киберпреступлений», — говорит господин Наместников.

При этом многие классификации киберугроз условны: в современных условиях бывает очень трудно отделить деятельность спонсируемой государством группировки от деятельности традиционных злоумышленников. ➔ 96