КИБЕРПРЕСТУПНОСТЬ
ПРИОБРЕТАЕТ ИНДУСТРИАЛЬНЫЙ ХАРАКТЕР

Хакеры-одиночки уступают место зрелым предприятиям

Тамаш Гайдош

В настоящее время киберпреступность представляет собой зрелую индустрию, функционирующую на принципах, весьма схожих с принципами законного бизнеса, стремящегося к извлечению прибыли. Бороться с распространением киберпреступности означает разрушить бизнес-модель, в которой используются легкие в применении инструменты для получения высокой прибыли при низком риске.

Хакеры-одиночки конца 1980-х годов, о которых ходили легенды (когда чужие компьютеры взламывались в основном для того, чтобы похвастаться навыками компьютерного аса 99-го уровня), канули в лету. Начавшаяся в 1990-е годы переориентация на получение прибыли постепенно стала доминировать в области хакинга и породила современную индустрию киберпреступности со всеми атрибутами обычного бизнеса, в частности, рынками, биржами, профильными операторами, поставщиками услуг на основе аутсорсинга, интегрированными цепочками поставок и так далее. Некоторые государства, используя такие же технологии, разработали высокоэффективное оружие для сбора разведывательных данных, промышленного шпионажа и разрушения уязвимой инфраструктуры противника.

Развитие

Киберпреступность распространяется, несмотря на то что предложение высококвалифицированных специалистов не поспевает за все более сложными технологиями, необходимыми для того, чтобы можно было безнаказанно совершать прибыльные взломы. Разрыв заполняется передовой инструментальной поддержкой и автоматизацией. За последние два десятилетия инструменты хакинга получили поразительное развитие. В 1990-е годы в этой профессии было популярно тестирование на возможность проникновения для обнаружения уязвимых мест компьютерных систем. Большинство доступных в то время инструментов были простыми, часто изготовленными на заказ, и их использование требовало серьезных знаний в области программирования, сетевых протоколов, внутренних компонентов операционных систем и различных прочих глубоко технических предметов. Как следствие, лишь некоторые профессионалы могли обнаружить недостатки, которыми можно было воспользоваться, и использовать их.

По мере усовершенствования инструментов и упрощения их применения менее умелые, но заинтересованные молодые люди (которых насмешливо называли «взломщики-дилетанты») начали сравнительно успешно их применять. Сегодня для того, чтобы запустить фишинг, то есть мошенническую практику отправления сообщения электронной почты, которое выглядит как сообщение от надежного отправителя, чтобы обманом заставить людей раскрыть конфиденциальную информацию, требуется только базовое понимание концепций, желание и немного денег. Совершать хакинг стало просто (см. рисунок).

Известно, что кибер-риск трудно оценить количественно. Данные об убытках скудны и ненадежны, отчасти из-за практического отсутствия стимулов к тому, чтобы сообщать о кибер убытках, особенно если инцидент не освещается широко в средствах массовой информации или отсутствует страхование от кибер-риска. Быстро меняющийся характер угроз делает данные прошлых периодов менее значимыми для прогнозирования будущих потерь.

Моделирование на основе сценариев, в котором определяются издержки, связанные с четко определенным инцидентом, затрагивающим экономику некоторых стран, дают оценки в десятки или сотни миллиардов долларов. Лондонская фирма Lloyd's оценивает убытки от отключения облачного сервиса, длящегося 2½–3 дня и затрагивающего страны с развитой экономикой, в 53,05 млрд долл. В процедуре моделирования МВФ средние совокупные годовые убытки в базовом сценарии составляли 97 млрд долл., в наименее благоприятном сценарии — в диапазоне 250 млрд долл.

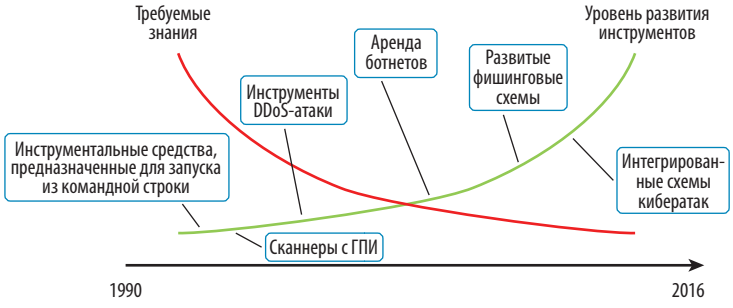
Причины и последствия

К совершению преступлений в физическом мире — с намерением получить деньги — как правило, побуждает просто прибыль, потенциально значительно более высокая, чем в случае законного бизнеса, что преступники расценивают как компенсацию за высокий риск. В мире киберпреступности схожая и даже более высокая прибыль возможна при значительно меньшем риске: там меньше вероятности

ИЛЛЮСТРАЦИЯ: ISTOCK / UGURHAN; YANREEEL

Проще простого

С повышением уровня развития инструментов хакинг требует меньше технических знаний, и в настоящее время совершить взлом значительно легче.



Источник: Carnegie Mellon University.
Примечание. DDoS-атака = распределенная атака типа «отказ в обслуживании»; ГПИ = графический пользовательский интерфейс.

того, что тебя поймают и успешно предадут суду, и почти полное отсутствие риска того, что в тебя будут стрелять. Рентабельность фишинга оценивается во многие сотни процентных пунктов, иногда она превышает тысячу. Можно только догадываться о том, получение какой прибыли стало возможным в результате краж интеллектуальной собственности, совершаемых наиболее изощренными киберзлоумышленниками. Основы, однако, схожи: эффективная инструментальная поддержка и исключительное отношение риска к вознаграждению служат убедительным аргументом и в конечном итоге объяснением резкого роста киберпреступности и ее превращения в индустрию.

Киберпреступность порождает системный риск в нескольких отраслях. Он по-разному затрагивает разные отрасли, но в то же время, вероятно, наиболее высок в финансовом секторе. Сравнительно новая угроза исходит от злоумышленников, нацеленных на разрушение. Стремясь дестабилизировать финансовую систему, они рассматривают наиболее перспективные мишени. Инфраструктура финансового рынка наиболее уязвима в силу ее важнейшей роли на мировых финансовых рынках. Поскольку финансовый сектор зависит от сравнительно малого набора технических систем, эффекты цепной реакции дефолтов или задержек вследствие успешных атак могут быть масштабными и иметь потенциально системные последствия.

Ввиду внутренней взаимосвязанности участников финансового сектора успешная дезорганизация платежной, клиринговой или расчетной системы — или кража конфиденциальной информации — приведут к масштабным вторичным эффектам и станут угрозой для финансовой стабильности.

К счастью, до настоящего времени мы не сталкивались с кибератакой с системными последствиями. Однако директивные органы и регулирующие органы финансового сектора все более осторожны ввиду последних инцидентов, которые вывели из строя сети банкоматов, и атак на системы банковского обслуживания в онлайновом режиме, центральные банки и платежные системы.

Финансовый сектор десятилетиями полагается на информационные технологии и имеет опыт поддержания надежной среды контроля за информационными технологиями, предписанной нормативными актами. При том что финансовый сектор, возможно, наиболее подвержен риску кибератак, такие атаки также связаны с повышенным риском для киберпреступников, отчасти из-за повышенного внимания к ним правоохранительных органов (такого же, как к старомодным ограблениям банков). Финансовый сектор также оказывает более эффективную поддержку правоохранительным органам, например, ведя обширную учетную документацию, представляющую ценность в судебных расследованиях. Более крупные бюджеты часто ведут к эффективным решениям в области кибербезопасности. (Заметное последнее исключение составляет компания Equifax, взлом которой произошел, пожалуй, вследствие того, что режим киберрегулирования был несоразмерен ее риску.)

В здравоохранении ситуация иная. За исключением наиболее богатых государств, здравоохранение, как правило, не располагает ресурсами, необходимыми для эффективной киберзащиты. Об этом свидетельствуют, например, совершенные в текущем году атаки с применением программ-вымогателей на компьютерные системы компании Allscripts, которая ведет электронные медицинские карты, и двух региональных больниц в США. Хотя здравоохранение также тщательно регулируется, и в отношении него действуют жесткие правила защиты данных, информационные технологии используются в нем далеко не так широко, как в финансовом секторе, и, как следствие, в нем не создана схожая культура жестких мер контроля за информационными технологиями. Это также делает здравоохранение более подверженным кибервзломам. Наибольшее беспокойство в связи с этим недостатком вызывает то, что, в отличие от финансового сектора, могут погибнуть люди, если, например, злоумышленники поразят компьютеризированные системы жизнеобеспечения.

В качестве следующих отраслей, в которых масштабные кибератаки могут иметь серьезные последствия, часто называют коммунальные системы, особенно энергосистемы и сети связи. В этом случае, однако, основные опасения вызывает разрушение систем государством-противником

или его проникновение в них напрямую или посредством представляющих его организаций. Как наглядно продемонстрировала массивная атака 2007 года на инфраструктуру интернета Эстонии, — которая парализовала финансовые услуги в онлайновом режиме, средства массовой информации и государственные ведомства, — чем более развита экономика и чем шире используется в ней интернет, тем более разрушительными могут быть кибератаки. Эстония входит в число обществ, в наибольшей мере перешедших на цифровые технологии в мире (см. «Взлет Э-стонии» в мартовском выпуске *Ф&Р* 2018 года).

Меры противодействия

В случае, если пострадает важнейшая инфраструктура, например, энергосистема, или телекоммуникационные и транспортные сети, или атака помешает правительству собирать налоги или предоставлять важнейшие услуги, могут наступить серьезные потрясения с системными экономическими последствиями, потенциально представляющие опасность для здоровья населения и безопасности. В таких случаях совокупный риск для глобальной экономики может превышать сумму рисков для отдельных лиц в силу глобального характера сетей и платформ информационных технологий, национального характера структур реагирования, неэффективности международного сотрудничества или даже присутствия государств среди злоумышленников.

Международное сотрудничество в борьбе с киберпреступностью и ее судебном преследовании значительно отстает от глобального характера этой угрозы. Наилучший способ борьбы с киберпреступностью — атаковать ее бизнес-модель, основанную на исключительном отношении риска к вознаграждению, связанном с неэффективным судебным преследованием. В этой связи должен быть значительно повышен коммерческий риск киберпреступности, но это возможно только в условиях более тесного международного сотрудничества.

Действия, связанные с киберпреступностью, могут охватывать несколько юрисдикций, что затрудняет их обезвреживание и судебное преследование. Некоторые юрисдикции борются с киберпреступностью медленно, неэффективно или просто не сотрудничают. Укрепление сотрудничества позволит ускорить и повысить эффективность розыска подозреваемых и предъявления им обвинений.

В финансовом секторе регулирующие органы разработали специальные стандарты оценки, установили обеспеченные правовой санкцией требования и целевые ориентиры и поощряют обмен информацией между компаниями и регулирующими органами и их сотрудничество. Органы банковского регулирования проводят проверки информационных технологий, в которых готовность к обеспечению кибербезопасности учитывается в стресс-тестах, планировании урегулирования и надзоре за надежностью и устойчивостью. Некоторые регуляторы для определения устойчивости к атаке требуют проведения имитационного моделирования кибератак, специально разработанных для каждой компании с использованием аналитической информации и экспертного потенциала государства и частного сектора. Компании также увеличивают инвестиции в кибербезопасность и включают готовность к обеспечению кибербезопасности в управление рисками. Помимо этого, некоторые компании стремятся перенести некоторые риски посредством страхования от кибер-риска.

Нынешний ландшафт кибербезопасности остается разнородным и децентрализованным: риски устраняются, главным образом, как местные идиосинкразические проблемы. Существуют некоторые механизмы сотрудничества, и правительства и регулирующие органы активизируют свои усилия, но выбор относительно кибербезопасности определяется в основном корпоративными потребностями — «каждому свое». Такая ситуация должна измениться, для того чтобы обеспечить в целом повышенную устойчивость к кибер-риску. Необходимы надежные превентивные меры как на уровне регулирования, так и на уровне технологий во всех отраслях. В число важнейших из них входит соблюдение минимальных стандартов кибербезопасности, обеспеченных скоординированной правовой санкцией регулирующих органов. Интенсивная подготовка кадров для повышения уровня информированности о кибербезопасности обеспечит защиту от базовых технических недостатков и ошибок пользователей, которые являются источником большинства взломов.

Кибератаки и нарушения кибербезопасности представляются неизбежными, поэтому также необходимо сосредоточиться на том, насколько оперативно мы выявляем взломы, насколько эффективно реагируем и насколько быстро возвращаемся в обычный режим деятельности. ФР

ТАМАШ ГАЙДОШ — старший эксперт по финансовому сектору Департамента денежно-кредитных систем и рынков капитала МВФ, является специалистом по кибербезопасности с более чем 20-летним опытом работы, в частности, по вопросам расследования банковских систем для обнаружения недостатков в их кибербезопасности. В прошлом он возглавлял Департамент надзора за информационными технологиями Центрального банка Венгрии.