22 → ПРЕСТУПНЫЕ ТЕХНОЛОГИИ

IT-угрозы делятся на две глобальных группы: технологические и человеческие. Вторые — самые распространенные. «Сейчас тех же вирусов крайне мало, основные вредоносные программы — трояны. Их особенность в том, что сами по себе они не распространяются: для их запуска нужна помощь пользователя — клик по ссылке, запуск программы. Именно пользователи бездумно открывают все подряд рассылки и посещают с рабочего места опасные сайты», — объясняет ведущий аналитик отдела развития компании «Доктор Веб» Вячеслав Медведев.

Появляются угрозы нового поколения, в которых приемы социальной инженерии становятся все более изощренными. «Сейчас в атаках используется предельно персонифицированная информация, которая убедит даже опытного пользователя, что сообщение отправлено ему лично. В результате, даже если используемая система защиты перенесет информацию в карантин, любой обнаруживший ее там будет уверен, что это ошибка и что данное сообщение нужно срочно отправить адресату», — делится технический директор Trend Micro в России Михаил Кондрашин.

Он рассказывает про новый вид атак — BEC (Business Email Compromise). Там вредоносный код вообще не используется: злоумышленники достигают своих целей, подделывая сообщения под распоряжения VIP-клиентов или руководства, например, с требованием срочного перевода денег по указанным реквизитам. «Несмотря на то, что такая атака кажется невероятно сложной, ущерб в мировом масштабе оценивается в миллиарды долларов. С учетом новых тенденций в любой организации необходимо внимательно рассмотреть каждый бизнес-процесс, приводящий к переводу денег наружу и проанализировать возможность его компрометации с использованием сообщений, выглядящих как несомненно подлинные, но не являющиеся таковыми», — призывает господин Кондрашин.

Генеральный директор компании «Атак Киллер» Рустэм Хайретдинов приводит такой пример: мотивированный на продажи клерк, чей профиль злоумышленники находят в соцсетях, получает письмо от потенциального покупателя, вкладчика или партнера. Письмо содержит, кроме безобидной и реально выглядящей информации о сотрудничестве, файл MS Office или PDF, зараженный вирусом. «Он атакует какую-нибудь безобидную систему, которую приходят чинить администраторы, при этом вводя свои пароли, которые перехватываются вирусом. Получив администраторский доступ к системе, вирус прописывает себя на платежном сервере и формирует платежи на заранее подготовленные компании», — описывает господин Хайретдинов.

Продвинутые способы краж обычно многоступенчатые, но сейчас все чаще применяются приемы социальной инженерии. В одной крупной компании службе безопасности на последнем этапе удалось пресечь перевод значительной суммы денег сотрудником, который имел право такие переводы осуществлять. «На сотрудника под видом одного из директоров C-уровня компании вышел злоумышленник, который стал писать ему письма, на протяжении продолжительного времени вел с ним переписку и, наконец, заручившись его полным доверием, попросил перевести на указанный счет крупную сумму денег, якобы для того, чтобы срочно закрыть большую сделку. Служба безопасности в последний момент распознала подозрительную активность и сумела предотвратить мошенничество», — поведал менеджер по продуктам Orange Business Services в России и СНГ Алексей Смирнов.

ЕВГЕНИЙ ПАВЛЕНКО

МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ ПОЗВОЛЯЮТ УБЕДИТЬ НЕИСКУШЕННОГО В ТЕХНОЛОГИЯХ СОТРУДНИКА ДОБРОВОЛЬНО СОВЕРШИТЬ ПРЕСТУПЛЕНИЕ

С помощью методов социальной инженерии современные хакеры вводят в заблуждение даже просвещенных сотрудников. «В нашей практике был случай, когда на электронную почту топ-менеджера компании пришло зловредное письмо, искусно замаскированное под резюме. Руководитель не просто скачал и открыл его, но и переслал в HR-отдел, запустив распространение вируса по сети компании. К счастью, именно в этот момент мы тестировали наши решения, и атака была предотвращена», — вспоминает технический директор Check Point Software Technologies Russia Никита Дуров.

Если вирус все-таки проникает в сеть, он может незаметно собирать необходимую информацию в течение месяцев. Действия хакеров могут развиваться по различным сценариям: они могут продать информацию конкурентам, заблокировать критически важные задачи и требовать выкуп, разместить на официальной странице компании компрометирующее сообщение.

«Еще более яркие примеры деструктивных последствий утечек мы наблюдаем в политике. Если коммерческая структура может обойтись штрафами, то репутационный ущерб для политика часто становится точкой невозврата. История с утечкой переписки Хилари Клинтон — яркое тому подтверждение», — замечает Лев Матвеев.

Атаки через мобильные устройства — это отдельное направление работы хакеров: исследователи Check Point почти каждый месяц находят новые уязвимости в операционных системах, приложениях и даже в чипах самих смартфонов. «Проблема в том, что современные мобильные устройства по сложности и функционалу сопоставимы, а иногда и превосходят обычные компьютеры, но люди до сих пор воспринимают их как обычные телефоны. Смартфоны открывают двери к банковским счетам пользователей, „умным“ домам, наконец, корпоративным данным. Очень сложно отследить действия сотрудников, которые используют свои личные гаджеты в рабочих целях. В их телефонах могут прятаться зловреды или боты-шпионы, фиксирующие контент, логины и пароли и персональные данные, которые могут повлечь серьезную утечку и корпоративных, и личных данных», — предостерегает Никита Дуров.

Заместитель директора по развитию бизнеса в России Positive Technologies Алексей Качалин упоминает об информационных угрозах, связанных с интернетом вещей. Их будет становиться все больше из-за роста этого сегмента и относительно низкого уровня защищенности подобных устройств. «Пока нет оснований ожидать его существенного роста: никто из производителей IoT-устройств добровольно не тратит время и средства на дополнительное тестирование своей продукции на наличие уязвимостей. Потому что это может поставить под угрозу первенство вывода продукта на рынок», — аргументирует господин Качалин. По его наблюдению, на рынке представлена масса уязвимых устройств, с помощью которых злоумышленники могут осуществлять даже глобальные атаки.

Компании просто обязаны иметь отработанные механизмы по выявлению кибератак и противодействию им, уверен руководитель IT-отдела компании «Актив» Сергей Сошников. «В первую очередь это резервное копирование и регулярные процедуры восстановления данных, постоянное обновление программного обеспечения. Это бизнес-критикал на текущий момент. Антивирусы, естественно, давно стоят на всех компьютерах. Они необходимы, но не являются панацеей в современном быстро меняющемся мире вредоносного программного обеспечения. Антивирусные базы обновляются часто, но вирусы меняют свои сигнатуры еще быстрее. Только возможность восстановления данных наряду с обучением сотрудников борьбе с социальной инженерией является лучшим методом отражения кибератак. Да, можно корпоративными политиками и правилами запретить персоналу пользоваться социальными сетями и публиковать в них информацию о работе, но с ростом количества сотрудников это становится неэффективным. Можно тренировать спам-фильтры и использовать продвинутые системы обнаружения угроз, но даже самые продвинутые из них зачастую не на 100% гарантируют фильтрацию опасного письма с вредоносной ссылкой», — утверждает Сергей Сошников.

БЕСПЕЧНЫЕ ЛЮДИ Глупых причин для IT-преступлений не бывает: все-таки это слишком серьезное нарушение, чтобы осознанно рисковать просто так. А вот случайных и нелепых утечек хватает, рассказывает Лев Матвеев. Согласно последнему исследованию его компании, в 2016 году на них пришлось 42% всех ИБ-инцидентов в российских компаниях. «Самая глупая утечка конфиденциальных данных случилась у одного из наших клиентов по вине сотрудника. Менеджер компании просто забыл ноутбук у клиента, оставил прямо на столе конференц-зала, где происходила встреча. В ноутбуке было много интересного: архив коммерческих предложений по отрасли заказчика, формулы формирования цены, архив догово-