УКРАСТЬ, НО НЕ ВЗЛАМЫВАТЬ

Заместитель начальника управления по раскрытию преступлений в сфере высоких технологий Министерства внутренних дел Беларуси Кирилл Вяткин рассказал, как изменились методы киберпреступников, что для компаний важнее, чем Apple Pay, и почему при разработке финтех-продукта нужно помнить про трех поросят.



Заместитель начальника управления по раскрытию преступлений в сфере высоких технологий МВД РБ Кирилл Вяткин

— Во всем мире рост количества киберпреступлений — привычная тенденция последних лет. Наша страна исключением не является. Если сравнивать с 2018 годом, число зарегистрированных злодеяний в сфере высоких технологий увеличилось более чем в два раза.

— Можно ли выделить какие-то тренды?

— Чаще всего совершаются хищения с использованием компьютерной техники. Преступники уходят от традиционной схемы — присвоения утерянной банковской карты или ее намеренной кражи для последующего снятия денег, оплаты товаров и услуг. Все понимают, что банкоматы и магазины оснащены камерами, значит, факт покупки или завладения средствами обязательно будет зафиксирован. Сейчас злоумышленники в основном предпочитают использовать реквизиты карточек при расчете в интернете — совершают операции в пределах суммы, не требующей ввода пароля, авторизации через 3D Secure и других аналогичных мер безопасности.

Еще один тренд — хищения с использованием систем дистанционного банковского обслуживания, жертвами которых становятся юридические лица. Преступления происходят по причине грубейшего пренебрежения вопросами информационной безопасности в организациях. Если работники не извлекают из компьютера ключ электронной цифровой подписи после совершения платежных операций через программу «Клиентбанк», злоумышленники имеют возможность, внедрив вредоносное ПО, получить удаленный доступ к системе и оформить перевод денег на подконтрольные счета.

Не сдают позиций фишинг и вишинг. Опробовав свои приемы в сопредельных государствах, преступники переключились на нашу страну и активно обогащаются, пользуясь доверчивостью белорусов. Деятельность злоумышленников так успешна, поскольку они хорошо изучили белорусский финансовый сектор и работают, что называется, с национальным колоритом.

мобильного телефона, реквизиты банковской платежной карты, остаток денежных средств на счету — сама по себе эта совокупность сведений не позволяет совершить хищение, но стоит только умело применить методы социальной инженерии, и дело принимает совершенно иной оборот. Персонализируя подход к каждой жертве, злоумышленники значительно увеличивают свои шансы добиться желаемого.

Незаконная торговля личной информацией в будущем приобретет еще большие масштабы. Согласитесь, преступнику проще купить готовую базу и спокойно ее отрабатывать, чем взламывать счета, ставить скимеры на банкоматы или распространять вирусы, которые крадут данные.

— В чем причины увеличения уровня преступности в сфере высоких технологий?

— Их две: активно прогрессирующий финтех-рынок и цифровая неграмотность населения. Внедрение инноваций как таковое, безусловно, на благо. К работе с клиентами теперь привлекают роботов, цифровые носители заменили бумажные, рассчитываться можно смартфонами, часами и кольцами. Финтех делает нашу жизнь в стиле smart. Теперь все просто: проснулся утром и в два клика решил свои вопросы. Все платежи одной кнопкой и никаких очередей в «сберкассу». Комфорт расслабляет: мы теряем бдительность, забывая о потенциальных угрозах и необходимости контролировать ситуацию.

Любой финтех-проект — прежде всего бизнес: во главу угла ставится выгода и получение максимального дохода при минимальном вложении времени и средств. В погоне за прибылью вопросы кибербезопасности уходят на задний план. Речь идет не только о ненадлежащей степени защиты персональных данных клиентов, но и уязвимости самих систем организаций в целом. К примеру, проблемы есть даже с разграничением доступа для пользователей-работников, хотя, казалось бы, каждому понятно, что носить все яйца в одной корзине — весьма сомнительная затея.

полагаться на поставщика технологии и считают, что как бы по умолчанию ограждены от преступных посягательств. В свою очередь злоумышленники целенаправленно отслеживают появление финтех-новинок, тщательно анализируют принципы их функционирования, выявляют слабые места, разрабатывают преступные схемы с элементами социальной инженерии и успешно завладевают чужими деньгами.



— Современные киберпреступники — кто они? Наверняка представление обывателей — гениальный хакер в темном капюшоне — безнадежно устарело?

— Действительно, раньше мы имели дело по большей части с людьми, получившими соответствующее образование, или талантливыми самоучками. Сейчас классические киберпреступники в основной своей массе

инструмент для этого по-прежнему разрабатывают и распространяют профессионалы, однако любой дилетант может получить доступ к нему с подробнейшей инструкцией по эффективному и безопасному применению в придачу. По этой причине «в профессию» пришло много людей, ранее судимых за имущественные преступления. Они поняли, что мир изменился. Теперь не нужно прислоняться к пассажирам в общественном транспорте, чтобы украсть кошелек. Гораздо проще позвонить потенциальной жертве, представиться работником банка, озвучить достаточно убедительный предлог и вынудить собеседника поделиться информацией, необходимой для хищения средств.

Другая категория — киберпреступники-инсайдеры. Это сотрудники организаций, обладающие широким кругом полномочий в силу служебных обязанностей и ведущие «подрывную деятельность» изнутри в интересах конкурентов, либо бывшие работники, которым после увольнения, в том числе по отрицательным мотивам, почему-то не закрыли доступ к коммерческой или иной важной для предприятия информации. Чтобы навредить бизнесу, они уничтожают данные или крадут их, не брезгуют шантажом и хищением средств со счетов юридических лиц.

— Получается, субъекты хозяйствования недостаточно эффективно обеспечивают свою защиту от кибер-угроз?

— Не думаю, что существуют организации, абсолютно пренебрегающие вопросами экономической безопасности, но вот что касается информационной — такая ситуация сплошь и рядом. Мы постоянно сталкиваемся с отсутствием у предприятий, даже очень крупных, какого бы то ни было локального нормативного акта, регулирующего политику информационной безопасности. В подобном регламенте должны быть закреплены организационно-правовые и технические меры реагирования на различные инциденты в сфере информационной безопасности, а также порядок взаимодействия с правоохранительными органами.

себя не должны. Нередки случаи, когда работники грубо нарушают информационную безопасность, но наказать за это невозможно, поскольку их не ознакомили с перечнем сведений, составляющих коммерческую тайну или относящихся к служебной информации ограниченного распространения. Иногда на предприятиях даже нет документов, предусматривающих какие-то санкции для провинившихся. Некоторым структурам проще внедрить Apple Pay, чем взять всех сотрудников на карандаш, организовать обучение правилам цифровой гигиены, провести пен-тест на уязвимость своего сайта или внутренней инфраструктуры. Необходимость этих мероприятий становится очевидной, когда ценная для компании информация с легкой руки злоумышленников превращается в бесполезный набор символов, а за дешифровку требуют десятки тысяч долларов.

Скажу больше: многие не подозревают, что стали жертвами киберпреступников. Буквально недавно столкнулся с подобной ситуацией: серьезная организация не знала, что база данных ее клиентов, а это несколько десятков тысяч белорусов, утекла в нелегальный доступ. Второй вариант — предприятие в курсе ЧП, но молчит о нем и к правоохранителям не обращается.

Настоятельно рекомендую повернуться к проблеме лицом. Наивно думать, что «уж моя-то фирма точно никому не сдалась». Поверьте, это всего лишь вопрос времени. В цифровом мире нельзя жить обособленно, как на острове. От киберпространства не отгородишься забором или шлагбаумом, оно открытое и безграничное. Для проверки белорусских организаций на прочность хакеру из Китая или США не нужно покупать билет, садиться в самолет, пересекать границу, проходить паспортный и таможенный контроль — достаточно выйти в интернет и попробовать на зуб все, что приглянется. К сожалению, в большинстве случаев попытка раскусить увенчается успехом.



правоохранительные органы не станут громогласно заявлять о неурядицах в какой-то компании, но если она работает с клиентами, то тут уже шила в мешке не утаишь. Люди общаются друг с другом, ничем не ограничены в своих высказываниях и имеют возможность комментировать ситуацию. В интернете множество площадок, где можно оставить отзыв о работе организации. Если нелестное мнение выскажет большое число пользователей, это повлечет за собой отток клиентов и потерю прибыли.

В общем, бизнес должен определиться со сценарием: соломенный финтех, который принесет какие-то деньги здесь и сейчас, но быстро схлопнется, или капитальное строительство добротного проекта с гарантированными долгосрочными перспективами. Кажется, выбор очевиден, но один знакомый банкир как-то сказал мне: «Мы посчитали: пока ущерб, нанесенный злоумышленниками, не превышает стоимость ликвидации выявленной уязвимости нашей системы, предпринимать что-либо не имеет смысла». Не сразу, но все-таки мне удалось убедить его в обратном.

сторонней компании для их проведения.

— Вероятно, самые защищенные и успешные финтех-продукты тоже не застрахованы от попадания в милицейские сводки?

— Именно так. Примерно два года назад в Беларуси появилась новая разновидность киберпреступлений — хищение денег абонентов сотовой связи через услугу банкинга, предоставляемую одним из мобильных операторов. Чтобы совершить подобное злодеяние, нужно на пару минут заполучить смартфон жертвы, к примеру, попросить позвонить. В несколько кликов на хозяина номера оформляется лимитированный микрозайм, сумма которого сразу выводится на подконтрольные злоумышленникам счета. Только спустя некоторое время владелец гаджета понимает, что должен возвращать деньги, которых не занимал.

Сам по себе мобильный банкинг — отличная технология, но люди оказались к ней не готовы. Никто не объяснил им, как правильно и безопасно использовать этот продукт. Мы обратили внимание мобильного оператора на проблему и стали вместе искать пути ее решения. В итоге систему усовершенствовали, минимизировав возможность противоправной деятельности в отношении клиентов.

Другой пример — услуга восстановления ПИН-кода банковской платежной карты посредством СМС. Казалось бы, очень удобно, однако подвох в том, что весь процесс можно произвести без участия законного держателя карты. В гостях, отелях, фитнес-клубах, да мало ли где еще наши телефоны и бумажники нередко остаются без присмотра. Воспользовавшись этим, преступникам ничего не стоит отправить сообщение, моментально получить в ответ четыре заветных цифры и дальше делать с этой информацией все, что душе угодно.

— Какие меры принимаются в республике для укрепления кибербезопасности финтех-отрасли и банковской сферы, а также

— Сам факт создания при Национальном банке Беларуси центра мониторинга и противодействия компьютерным атакам в кредитно-финансовой сфере FinCERT свидетельствует о пристальном внимании государства к актуальным вопросам и проблемам информационной безопасности в этой области. Отлично, что теперь в процессе оценки защищенности внедряемых технологий и реагирования на киберинциденты участвуют не только правоохранительные органы. Как ни крути, отношения внутри банковской сферы более тесные и доверительные, чем со сторонними структурами. В таких условиях гораздо проще оперативно выработать по-настоящему уместное и действенное решение для каждого конкретного случая, а затем осуществить грамотную координацию взаимодействия всех заинтересованных сторон в ходе его реализации. Подобный консолидированный подход поможет снизить мотивацию злоумышленников, сведя к минимуму возможность отыскать новую лазейку для совершения киберпреступлений.

Следует отметить, что органы внутренних дел также непрерывно совершенствуют организационные и практические меры по борьбе с киберпреступностью: меняется оргштатная структура подразделений по раскрытию преступлений в сфере высоких технологий, обновляется техническое вооружение, растет профессиональный уровень стражей порядка, развивается международное сотрудничество правоохранителей. Кроме того, во многих крупных территориальных органах внутренних дел уже есть высококвалифицированные борцы с киберпреступностью, в компетенцию которых входит исключительно реагирование на киберинциденты и работа с пострадавшими в них.

