CINEMA

CYBERD0CUMENTARY

12/12/2017

КИБЕРБЕЗОПАСНОСТЬ 2017–2018: ЦИФРЫ, ФАКТЫ, ПРОГНОЗЫ

POSITIVE TECHNOLOGIES

Содержание

Введение

Прошедший год стал поучительным для бизнеса в контексте информационной безопасности. Выражение «лучше один раз увидеть, нежели сто раз услышать» — как раз о нем. Столкнувшись с вирусами-шифровальщиками, компании прочувствовали на себе важность элементарных правил ИБ-гигиены. Отсутствие актуальных обновлений и привычка жить с уязвимостями привели к остановке заводов Renault во Франции, Honda и Nissan в Японии; пострадали банки, школы, энергетические, телекоммуникационные компании; только лишь одна компания Maersk потеряла 300 млн долларов. На фоне информационного цунами, вызванного вирусами-вымогателями, некоторые важные события остались за пределами массового внимания. Перед тем, как изложить наши прогнозы на 2018 год, перечислим основные реперные точки минувших 12 месяцев в мире кибербезопасности:

Практическая безопасность
С бумажной безопасностью начали бороться на самом высоком уровне. Федеральный закон N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» не просто рекомендует, а обязывает компании различных отраслей (как государственные, так и коммерческие) защищаться и вводит механизмы контроля эффективности защитных мер.

Уязвимости SS7 заметили
Злоумышленники начали перехватывать коды для двухфакторной аутентификации с помощью уязвимостей сигнального протокола SS7. Первыми пострадали абоненты O2-Telefonica.

«Масштабируемые» атаки на банкоматы
Банкоматы грабят давно и разными способами, например, привязывают к тросу автомобиля и увозят. Но когда киберпреступники стали подключаться к локальной сети банка и удаленно контролировать множество АТМ, у банков появился серьезный повод для беспокойства.

Тайный майнинг
Весной 2017 года наши эксперты обнаружили сотни компьютеров в крупных компаниях, которые майнили криптовалюту для неизвестных взломщиков. Майнер использовал ту же уязвимость, что и WannaCry, и защищал от шифровальщика захваченные ПК.

Войти через IoT
Не успел стихнуть шум вокруг безопасности IoT из-за ботнетов и DDoS-атак, как с помощью незащищенных «умных» кофемашин стали останавливать нефтехимические заводы, а смарт-аквариумы использовать для атак на казино.

Биткоины и уязвимый веб
К концу года биткоин опередил по капитализации российский рубль, и хакеры сконцентрировали свое внимание на блокчейн-стартапах. Самая простая схема атаки стала наиболее популярной — найти уязвимости на сайте ICO и подменить адрес кошелька для сбора инвестиций. Израильский CoinDash таким образом лишился $7,5 млн.

Эпидемия целевых атак
Число компаний, столкнувшихся в 2017 году с APT-атаками, увеличилось почти вдвое. Одновременно с этим атаки прямо на глазах усложняются, начинают активно применяться методы, затрудняющие анализ и расследование инцидентов.

Рынок ИБ: общие тренды и драйверы

Сектор ИТ в совокупности по публичным оценкам ежегодно демонстрирует рост до 10%. В этом году и **кривая объема рынка ИБ пошла вверх: по нашим оценкам, в этом году он покажет рост до 15%** (в деньгах заказчика), а по итогам следующего, 2018, этот показатель может оказаться и еще выше. Причина этому в том числе и в резко возросшем интересе организаций к реальной безопасности, спровоцированном:

- **громкими публичными инцидентами последних 1,5—2 лет**, которые привлекли внимание руководства компаний к роли информационной безопасности в жизнеспособности бизнеса (по экспертной оценке Positive Technologies каждый пятый топ-менеджер сегодня так или иначе проявляет интерес к практической безопасности применительно к своему бизнесу);
- **сформировавшимся личным опытом отечественных компаний**, демонстрирующим на практике последствия пренебрежения гигиеной информационной безопасности. Здесь мы имеем в виду нашумевшие эпидемии WannaCry, NotPetya, BadRabbit, показавшие, что фокусировка на сложных технологических решениях при игнорировании азбучных истин (к примеру, необходимости своевременного обновления ПО) могут иметь фатальные последствия;
- **принятым на уровне государства курсом на цифровую экономику**, охватывающим все сферы (от здравоохранения и образования до транспорта и финансов), что сказывается на росте сектора ИТ в целом и сфере информационной безопасности в частности.

В течение 2017 года сформировался и ряд тенденций, играющих определяющую роль в ведении бизнеса в сфере ИБ в целом:

- во-первых, стала явной сегментация рынка с точки зрения подходов к обеспечению безопасности: **четко сформировался пул компаний, осознающих прямую зависимость между жизнеспособностью своего бизнеса и ИБ**. Это те компании, которые выстраивают свою работу с акцентом на диджитализацию. Именно они инвестируют в новейшие технологии защиты и во многом подталкивают прочих игроков рынка к обеспечению безопасности нового типа. Таких компаний пока немного и преимущественно это организации финансового и телекоммуникационного секторов. Тем не менее, на их долю приходится около 10% рынка в целом и их число растет;
- во-вторых, **на основе блокчейн-технологий формируется новая бизнес-среда**, которая ставит игроков рынка в условия, требующие гораздо большей оперативности и гибкости от всех участников процесса. Например, цикл продажи сокращается с месяцев до пары-тройки дней, в том числе заставляя нас, как поставщиков сложных, тяжелых средств защиты, разворачивать их за сутки и даже часы. Это новый подход к бизнесу, где во главе угла стоят технологии (в том числе и технологии защиты, так как они приобретают ключевую роль в обеспечении бизнес-процессов). По такому пути уже начали идти и некоторые гиганты отечественного крупного бизнеса (пока их единицы). Так или иначе жизнь в новых технологиях заставит крупный бизнес, особенно связанный с ритейлом или предоставлением услуг (банковских, телекоммуникационных и пр.), стать более динамичным, соответствующим новым принципам;
- в-третьих, **общая тенденция на практическую безопасность** нашла свое отражение и в законотворческих инициативах. Например, в этом году вышел Федеральный закон N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который отрасль ждала почти пять лет, и ряд других нормативных документов. Все они в первую очередь об обеспечении реальной защищенности, то есть рынок отказывается от подхода, основанного на формальном соответствии законодательным требованиям, в пользу реальных практик обеспечения защиты.

В числе технологических тенденций, которые, сформировавшись в 2017 году, будут активно влиять на сферу ИБ в ближайшие годы, стоит отметить:

- резко **возросший интерес к мониторингу и выявлению инцидентов ИБ**: мы наблюдаем смену парадигмы защиты от так называемого «построения заборов» вокруг инфраструктуры, к более гибкой и интеллектуальной задаче «выявления киберпреступника или его активности» в инфраструктуре;
- сфера аутсорсинга ИБ развивалась на протяжении последних 5–7 лет, однако по-настоящему переломными для нее стали последние год–полтора: сегодня **аутсорсинг в сфере информационной безопасности — более чем очевидная тенденция**. Причина все в тех же реальных инцидентах ИБ, число которых резко возросло в последнее время. Для эффективного противодействия им, помимо технологической базы, необходимы еще и высококвалифицированные (а подчас и очень узкоспециализированные) эксперты, число которых на рынке ограничено и большая их часть аккумулируется сегодня компаниями-аутсорсерами. Учитывая, что активность киберзлоумышленников тенденции к снижению не показывает, то востребованность экспертизы аутсорсеров будет только расти;
- **на порядки увеличившийся объем информации, который ИБ-специалисту необходимо обрабатывать и анализировать «на лету»** (всевозможные фиды, индикаторы компрометации, оповещения, события и пр.), ставит нас еще перед одним технологическим вызовом: эффективная обработка разрозненных и часто явно не связанных друг с другом данных (своего рода «большие данные» - Big Data - информационной безопасности) с последующим анализом и оценкой рисков. Те, кто научится аккумулировать эти данные, хранить их, гибко обрабатывать и анализировать (в том числе ретроспективно), окажутся в прямом смысле слова «царем горы» на нашем рынке на ближайшие несколько лет.

Эволюция кибератак

2017 год позволил нам выявить три основных тренда в области подходов к атакам на организации, которые будут весьма актуальны и в ближайший год:

- **всплеск популярности деструктивных массовых атак**, когда злоумышленники нацелены на как можно более масштабный охват и причинение ущерба. Как это было, например, в случае с NotPetya, WannaCry (или другими шифровальщиками), которые прокатились по миру в этом году. Иногда логика работы вредоносного ПО даже не подразумевала возможность расшифровывания данных, а используемые методы распространения были настолько эффективными, что позволили заражению в считанные часы распространиться по всей планете. Если в 2015–2016 годах подобных атак практически не было (исключением являлись, пожалуй, лишь атаки на IoT, например, создание ботнета Mirai и DDoS-атаки, проводимые с его помощью), то в 2017 году, по экспертной оценке Positive Technologies, каждая 10-я организация столкнулась с вирусами-шифровальщиками;
- применявшийся ранее метод отправки писем с простой подменой адреса отправителя стал встречаться реже – большая часть фишинговых писем начала блокироваться спам-фильтрами на почтовых серверах, и такая рассылка стала требовать большего внимания к доставке писем, прохождению ими фильтров на почтовых серверах. Поэтому **злоумышленники** изменили тактику и **теперь активно атакуют поставщиков и контрагентов компаний, для того чтобы использовать их инфраструктуру и учетные записи реальных сотрудников для развития атак на другие организации**. Подобная тактика уже использовалась злоумышленниками, например, когда через инфраструктуру компании M.E.Doc нарушители распространили вирус NotPetya, который заблокировал рабочие станции во многих крупных организациях. Также подобный подход довольно часто использует группировка Cobalt, которая специализируется на атаках на финансовый сектор, производя взлом контрагентов банков, а уже потом от их имени осуществляя атаки на сами банки. Схожая ситуация сложилась и в истории с заражением вирусом BadRabbit, когда злоумышленники предварительно были нацелены на инфраструктуру легитимных новостных ресурсов, с которых далее происходила «раздача» вредоносного ПО. В среднем каждая вторая успешная атака на организацию, которую расследовал экспертный центр безопасности (Expert Security Center) компании Positive Technologies в

течение 2017 года, была проведена через скомпрометированный «ранее надежный» источник;

- **общий рост числа APT-атак** (таргетированных, целевых) на организации: общее число компаний, столкнувшихся в 2017 году с APT-атаками, увеличилось почти вдвое – каждая вторая крупная организация обнаружила следы присутствия злоумышленников в своей инфраструктуре. При этом среднее время присутствия злоумышленника в инфраструктуре по-прежнему составляет три года. На общую статистику влияют два момента: во-первых, в информационном пространстве увеличилось число высококвалифицированных и технологически оснащенных кибергруппировок, а во-вторых, общий рост процента атак данного типа вызван еще и тем, что государственная политика в области ИБ все больше и больше требует от владельцев информационных инфраструктур (особенно критических) выстраивать корректные процессы по выявлению, реагированию и локализации компьютерных инцидентов с использованием правильных технологий. Поэтому мы видим не только общий количественный рост выявленных случаев APT-атак, но и рост числа самостоятельных обнаружений таких фактов организациями (пока незначительный – до 10%). При этом надо понимать, что стартовавший процесс создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), в рамках которой необходимо будет сообщать о компьютерных инцидентах, организовывать процессы их выявления и реагирования на них, в ближайшие 1–2 года приведет к всплеску публичной статистики о различных таргетированных атаках на коммерческий и государственный сектор.

Еще один момент, который необходимо отметить, – **усложнение атак с технологической точки зрения**: злоумышленники стали активно использовать методы, затрудняющие анализ и расследование инцидентов. Используются так называемые средства анти-анализа, анти-атрибуции, анти-форенсики, увеличилось число бесфайловых атак, вредоносное ПО все чаще стало подписываться цифровыми подписями и пр. С течением времени атаки будут только усложняться, во многом благодаря и утечкам архивов АНБ: опубликованные в них техники и тактики активно используются и при необходимости модифицируются злоумышленниками. Существенно сокращается окно между появлением новой технологии и принятием ее на вооружение злоумышленниками: в среднем между появлением нового эксплойта и началом активного его использования злоумышленниками проходит от 3 до 5 дней. А некоторые, особо продвинутые группировки, ориентированные на получение финансовой выгоды (такие, например, как Cobalt) тратят на адаптацию новых эксплойтов и техник и их применение в своих атаках всего лишь несколько часов.

Все это требует от организаций большей гибкости и оперативности в отслеживании новейших угроз и методов атакующих, использования более «интеллектуальных» средств защиты, обеспечивающих минимальное отставание от тактик нападающих. Ответом на это стал рост интереса к таким направлениям ИБ, как Threat Intelligence, Threat Hunting, Incident Response, а также к созданию центров мониторинга безопасности (SOC): только в этом году около 10 компаний приступили к созданию своих SOC в той или иной форме, в 2018 году их число, по нашим прогнозам, вырастет в три раза.

Регулирование отрасли ИБ

Фактически **вся вторая половина 2017 года прошла под знаком Федерального закона N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»** – это первый в России случай, когда вступает в силу закон, охватывающий широчайший спектр отраслей единовременно (банковская сфера, связь, здравоохранение, наука, промышленность и т.д.). Это первый прецедент, когда закон не просто дает регуляторные рекомендации, а обязывает реально защищаться от компьютерных атак, вводит оценку требований и механизмы защищенности критических информационных систем. Выполнение закона будут регламентировать ФСТЭК России, который устанавливает требования безопасности и проверяет их исполнение, и ФСБ России, в чьи полномочия входит оценка реальной защищенности информационных систем, проведение расследований компьютерных атак (когда они затрагивают интересы государства), помощь в реагировании на атаки, т.е. выработка подходов к

защите от принципиально новых атак. Также закон предусматривает уголовную ответственность для владельца недостаточно защищенной информационной системы.

Сформировалась новая для российского рынка концепция «частно-государственного» партнерства в области безопасности. Данная схема предполагает наличие государственных или частных систем, которые нужно защищать. Во главе схемы располагается государство в лице 8 центра безопасности ФСБ России, которое отвечает за функционирование системы ГосСОПКА, и есть разнообразие корпоративных и ведомственных центров реагирования на компьютерные атаки. В результате получается, что общегосударственная защита информационных систем распределяется между государством и коммерческими компаниями. При этом появляется возможность реализовывать аутсорсинг информационной безопасности. В конечном счете создается система взаимосвязанных субъектов: защищающиеся системы, ГосСОПКА, государство. Система ГосСОПКА и требования закона N 187-ФЗ не гарантируют, что систему невозможно будет взломать, но выполнение этих требований и **создание центров ГосСОПКА позволит отсечь 90% примитивных атак**, позволив сконцентрироваться на высокоуровневых.

Создание процесса предупреждения компьютерных атак и реагирования на них – длительная и циклическая задача, разбивающаяся на несколько простых этапов: компании необходимо поставить цель защититься от тривиальных атак и атак низкой сложности (по статистике это примерно 75% атак). Только решив эту задачу, можно переходить к защите от более сложных атак, а затем - от незнакомых типов атак. Стоит особенно отметить, что закон нацелен на практическую безопасность: не идет речи о выполнении каких-то требований, наоборот, ставится задача грамотно реагировать на определенные компьютерные атаки.

Мировая практика также близка к российскому стилю регулирования в сфере кибербезопасности. Например, закон о защите персональных данных (GDPR), вступающий в силу в 2018 году в Евросоюзе, определяет, насколько система является значимой для субъекта обрабатываемых персональных данных. Для значимых информационных систем вводятся привычные нам понятия: национальное регулирование, сертификация систем на требования национальных регуляторов. От добровольной защиты информационных систем западный мир переходит к императивным подходам, т.е. обязательным требованиям по защите информации. Таким образом, и российский и зарубежный рынок сейчас задаются одним и тем же вопросом: что мы должны сделать, чтобы привести свою систему защиты к соответствию с новыми видами законодательства.

Банкоматы и платежные системы

Статистика компании Positive Technologies позволяет утверждать, что **в течение всего 2017 года финансовые компании входили в пятерку наиболее атакуемых киберпреступниками типов организаций**. При этом киберпреступники в этом году сосредоточились на использовании таких схем, которые:

- легкодоступны (с использованием инструментария и инструкций, которые можно приобрести относительно недорого и без лишних сложностей);
- масштабируемы: такие схемы всегда пользовались среди злоумышленников большим спросом, так как если схему невозможно масштабировать – она скорее всего потеряет свою актуальность буквально уже после нескольких первых атак;
- успешно (а главное быстро) монетизируются.

Всем этим трем пунктам удовлетворяют, например, **атаки на АТМ (так называемые логические атаки на банкоматы)**. Этот тип атак демонстрирует драматический рост в этом году: только за первое полугодие 2017 года общий объем атак такого типа в странах Европы вырос на 500%. В России и странах СНГ число атак такого типа также показывает динамику роста, и целями становятся крупные игроки банковского рынка.

Сегодня атака на АТМ превратилась из подхода, доступного единицам злоумышленников, в своего рода массовый рынок— отработанную и растиражированную методологию с инструкциями и доступным инструментарием: имеется достаточное число вариантов вредоносного ПО для джекпоттинга (заражения банкомата вредоносным ПО, провоцирующим управляемую выдачу денег) и

инструментов для BlackBox-атак[1]. Сегодня злоумышленник за несколько тысяч долларов может приобрести полный комплект инструментария на черном рынке, а далее ему остается лишь выбрать банкомат, опустошить его, следуя инструкциям, и искать следующий. Надо понимать, что затраты окупаются очень быстро: буквально за несколько успешных атак. И данная тенденция в целом сохранится до тех пор, пока и банки, и производители банкоматов и средств защиты не придут к массовому внедрению эффективного решения по защите.

У сложившейся ситуации несколько причин. Во-первых, **АТМ отличаются крайне низким уровнем защищенности в целом**: в части защиты от атак типа BlackBox и защищенности операционных систем банкоматов в принципе. Наши работы по аудиту, проведенные за последние два года, показывают, что при наличии доступа к компьютеру банкомата в 85% случаев удается извлечь из него деньги, а при наличии возможности выполнения хотя бы ограниченного списка команд – в 100%.

Во-вторых, **большинство представленных сегодня на рынке средств защиты недостаточно эффективны** (в том числе и такие, как McAfee Solidcore, официально рекомендованный компанией NCR). Только за последний год исследователями Positive Technologies в 5 разных продуктах класса Application Control было выявлено 9 уязвимостей, позволяющих получить максимальные привилегии на банкомате или обойти это средство защиты (удаленно или локально). Причем опыт исследователей показывает, что задача обойти средства защиты класса Application Control решается буквально в течение недели. Это означает, что в реальном мире злоумышленник справится с этим в сравнимые сроки.

Ну и в-третьих, **сами производители средств защиты проявляют недостаточное внимание к сообщениям исследователей о выявленных в их продуктах уязвимостях**: доля вендоров, игнорирующих сообщения исследователей о выявленных уязвимостях (или реагирующих на них в сроки, превышающие разумные 90 дней ответственного разглашения), остается удручающе велика – в среднем не более 70% выявленных нами проблем, так или иначе связанных с банкоматным ПО или «железом», признаются и закрываются разработчиками.

В 2017 году **банки также стали проявлять интерес к защищенности POS-терминалов, платежных систем нового типа (Apple Pay, Samsung Pay и пр.), а также к эффективности своих антифрод-систем** – данный интерес выражается в росте запросов на аудиты безопасности перечисленных систем и устройств.

Что нас ожидает: среди киберпреступников сохранит актуальность популяризация рабочих схем (чем больше схема отвечает трем требованиям – доступность, масштабируемость, монетизируемость, — тем выше шанс ее превращения в массовую). Банки, в свою очередь, станут еще активнее интересоваться реальными угрозами (грозящими финансовыми потерями) и оценивать риски.

Телекоммуникационные сети и IoT

Более пяти лет подряд мы говорим о проблемах безопасности мобильных сетей, в частности – об уязвимостях SS7. Нас часто спрашивают, когда же телекоммуникационные компании научатся защищать этот протокол или, наконец, заменят его на более безопасный?

Выбором средств защиты обеспокоены как зарубежные, так и российские операторы. Кроме того, сейчас большинство операторов использует сети LTE, где на смену стеку протоколов SS7 пришел иной протокол — Diameter. Согласно статистике аналитического агентства Ovum, по итогам второго квартала 2017 года в мире осуществляется больше подключений к сетям LTE, нежели к сетям 3G. Приведем цифры, актуальные для второго квартала 2017 года:

- 2,36 млрд — число пользователей LTE по всему миру.
- 878 млн — число LTE-подключений за последние 12 месяцев.
- 59% — рост количества LTE-абонентов за год.
- 30% — доля LTE-абонентов от общего числа подключений.

[1] Blackbox атака — одна из самых распространенных jackpotting-атак направленная на прямую выдачу наличных средств из SDC/USB и RS232 диспенсеров путем подключения внешнего контроллера к шине передачи данных. В настоящий момент, данный вид атаки повсеместно используется на все территории РФ и Европы и является прямой угрозой финансовой безопасности банков так как зачастую потери не покрываются страховкой.

В прошлом году мы провели исследование безопасности протокола Diameter, в рамках которого обнаружили, что **каждая исследованная нами сеть 4G на базе Diameter обладала аналогичными с устаревшим протоколом SS7 уязвимостями**. Используя их, злоумышленник может вести слежку за абонентом, перехватывать SMS-сообщения в целях взлома аккаунтов онлайн-банка, социальных сетей и т.п.

Помимо традиционных угроз в последнее время в обществе активно обсуждается **тема развития «умных городов»**. В рамках нашей темы необходимо отметить, что жизненно важные системы для таких городов — светофоры, дороги, коммунальные услуги - будут управляться через мобильные сети LTE, это следующий этап развития мобильных сетей LTE — LTE-M, 5G. Однако атаки через уязвимости мобильных сетей могут полностью парализовать работу «умного города». К 2025 году в России планируется создать 50 «умных» городов, а уровень информатизации общественного транспорта достигнет 100%.

Уязвимые мобильные сети связывают **миллионы «умных» устройств, которые рано или поздно могут «сойти с ума»**. По данным экспертов, к 2020 году число IoT-устройств, подключенных к сотовым сетям, увеличится с 400 млн до 1,5 млрд. Бурное проникновение «умных» устройств в бизнес и повседневную жизнь — еще один повод задуматься о безопасности мобильных сетей. IoT-устройства проникают не только в наш дом, но и в производство, добывающую промышленность и энергетику. Человек принимает минимальное участие в их работе: машины общаются с друг другом, принимая решения без его участия. В таком случае компрометация даже одного «умного датчика» может привести к непредсказуемым последствиям. Наши исследования показывают, что мир Интернета вещей имеет разную степень защищенности: от надежно защищенных устройств до откровенно «дырявых», с помощью которых злоумышленник может наблюдать, что происходит у вас дома.

Результат аудитов «умных домов» показывает, что **самым уязвимым устройством является видеокамера**: злоумышленник может получить к ней полный доступ и использовать для слежки, проникновения в сеть, подмены видеопотока. Примером может стать наше недавнее исследование безопасности камер Dahua, в рамках которого мы установили и помогли устранить критическую уязвимость во встроенном ПО. Такие камеры широко используются для видеонаблюдения в банковском секторе, энергетике, телекоммуникациях, транспорте, системах «умный дом» и других областях. Уязвимость позволяет сделать с камерой все, что угодно: перехватить и модифицировать видеотрафик, включить устройство в ботнет для осуществления DDoS-атаки и многое другое. Кроме того, беспроводные датчики, входящие в состав умных домов, не всегда используют шифрование, поэтому могут быть использованы злоумышленником для выведения всей системы умного дома из строя.

Самоуправляемые автомобили также находятся под угрозой. С помощью мобильных сетей автомобили обмениваются данными о скорости, расположении автомобилей на трассе и пр. DDoS-атаки могут оставить такой автомобиль буквально без «чувств и глаз». Машины не смогут обновлять информацию о дорожной ситуации. Таким образом, уязвимости мобильных сетей могут стоить не только больших денег, но и человеческих жизней.

Если сейчас пользователи могут повлиять на безопасность устройства, правильно настроив роутер и доступ к устройству извне, то в случае использования мобильных операторов все будет полностью зависеть от защищенности мобильных сетей, которая как мы знаем, сейчас оставляет желать лучшего.

В течение прошедшего года мы принимали активное участие в работе отраслевой организации операторов мобильной связи (GSMA). В рамках рабочих групп наши эксперты обратили внимание мобильных операторов на небезопасности протокола Diameter. Благодаря этому **операторами было принято решение об отказе от протокола Diameter в сетях следующего поколения 5G и замены его на альтернативный вариант**. Нами также ведется активная работа над поиском решений повышения защищенности IoT-устройств. Среди первоочередных шагов мы рекомендуем следующие:

- отказ от небезопасных протоколов, фильтрация пользовательского ввода адресов и данных;
- введение парольных политик, регулярные обновления;
- отключение отладочных механизмов (JTAG), физическая защита устройств;
- использование HTTPS, двухфакторной аутентификации;

- аудит защищенности;
- практика безопасной разработки с использованием анализаторов кода;
- внедрение отраслевых и государственных стандартов безопасности — по аналогии с промышленными системами управления (АСУ ТП).

Если ситуация с безопасностью мобильных сетей и IoT-устройств не изменится, первыми под удар попадут те сервисы или службы, для которых отказ в обслуживании будет наиболее чувствительным: в качестве примера можно назвать умные светофоры, подключенные к мобильным сетям, уязвимости которых могут в конечном счете стать причиной транспортного коллапса или аварии.

Блокчейн-технологии и смарт-контракты

Исследовать технологию блокчейн эксперты Positive Technologies начали летом 2017 года и уже к сентябрю появилась услуга по защите ICO. За два месяца было выполнено около десяти проектов для компаний различных отраслей, в том числе банков.

Наиболее частый недостаток в смарт-контрактах — несоответствие стандарту ERC20, который описывает интерфейс токена[2] для кошельков и криптобирж. Если стандарт реализован в токене неправильно, то это может привести к неожиданным результатам вплоть до невозможности торговли и переводов. Существуют и другие угрозы, перечислим **топ-3 векторов атак**:

- **Frontrunning** (или из биржевой терминологии «**опережающий бег**») позволяет предугадать будущее состояние контракта в момент, когда целевая транзакция еще не замайнена, т.е. не попала в блок. Атакующий может подсмотреть эту транзакцию и выпустить свою таким образом, чтобы она попала в тот же блок, но перед целевой. Например, это позволяет предугадать случайное число, которое отправляется в контракт извне. Либо получить прибыль с токенов в момент, когда происходит большая покупка. Например, проект Bancor был подвержен frontrunning, из-за которой была возможность иметь преимущество, если кто-то совершал большую покупку токенов;
- **Неверное определение области видимости**. Из-за этой уязвимости в июле 2017 года была совершена кража около 30 миллионов долларов с кошелька Parity, на котором хранились средства множества клиентов, включая несколько крупных ICO-проектов. Уязвимость была возможна из-за того, что функция, которая устанавливает владельца кошелька, была доступна для вызова любому пользователю платформы Ethereum. Разработчик использовал один из шаблонов, но применил его неправильно, не указав область видимости функции;
- **Неправильная генерация случайных чисел** — случай с лотереей SmartBillions. Разработчики выложили код контракта и пополнили баланс кошелька лотереи на 1500 эфира (это примерно полмиллиона долларов). Создатели были настолько уверены в своем коде, что объявили багбаунти[3]: любой, кто сможет найти уязвимость в коде, может забрать все средства себе. И буквально через два дня с кошелька начали совершаться странные транзакции по 200 эфира — выяснилось, что контракт содержал ошибку, о которой предупреждает документация. Кто-то смог воспользоваться этой ошибкой и предугадать случайное число.

Также наша команда проверяет соответствие whitepaper — технического документа, описывающего продукт или технологию, и экономику ICO. Под экономикой ICO имеются в виду этапы ICO, распределение полученных средств, стоимость одного токена, планка soft cap (т.е. минимальная сумма, при которой ICO считается успешным, если она не достигается, то должно производиться возмещение средств инвесторам) и пр. Если в контракте не выполняются пункты, заявленные в whitepaper, то мы также включаем это в отчет.

Безопасность ICO не ограничивается контрактами, есть множество других путей взлома. Например, у одного из наших заказчиков мы смогли получить доступ к критически важной почте, так как у генерального директора был простой контрольный вопрос для восстановления доступа. В другом проекте мы смогли зарегистрировать свой сайт на том

2 Токен — компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удалённого доступа к информационным ресурсам и т. д.

3 Программа Bug Bounty — это программа, предлагаемая многими веб-сайтами и разработчиками программного обеспечения, с помощью которой люди могут получить признание и вознаграждение за нахождение ошибок в программном коде, особенно тех, которые касаются эксплойтов и уязвимостей.

же хостинге, что и целевой, и через уязвимость в самом хостинге нам удалось добраться до сайта ICO и получить контроль над ним.
Необходимо быть готовым ко всему: злоумышленники могут подменить на сайте ICO адрес кошелька для сбора средств на свой, зарегистрировать похожий адрес с целью фишинга, начать DDoS-атаку и многое другое.

Защита ICO — это целый комплекс мер, который не ограничивается лишь аудитом смарт-контракта. Каждый ICO-проект должен иметь своего рода чеклист (список обязательных пунктов) безопасности, куда должен входить анализ исходного кода веб-приложения, так как взломав веб-сайт, злоумышленники смогут подменить адрес контракта. Должен проводиться аудит инфраструктуры в режиме черного ящика, так как даже если в коде веб-приложения уязвимостей нет, его могут взломать через соседние сайты или уязвимость сервиса. Сегодня перед запуском ICO скупают порядка 200 доменов в разных зонах, иначе злоумышленники сделают это за вас и начнут рекламную кампанию в поисковиках. Не рекомендуется использовать мессенджер Slack, так как в нем есть возможность создавать свои каналы внутри команды, чем могут воспользоваться фишеры. Необходимо проверять настройки безопасности почтового сервера, иначе начнутся спам-рассылки от имени ICO. Важно настроить двухфакторную аутентификацию, проверить публично доступную информацию о команде ICO, ну и, конечно же, нигде не использовать простые пароли.

По данным ForkLog, в 2017 году уже прошло более 300 токенсейлов[4], т.е. примерно по одному в день. За первые три квартала 2017 года ICO-проекты собрали около $3 млрд. Доля ICO, не достигших своей цели, возрастает: в июне это было 7% проектов, в августе 54%, в сентябре 66%. Данная тенденция будет наблюдаться и в следующем году.

Что касается технической части, то **в 2018 году платформу Ethereum скорее всего затронут серьезные изменения**. Вышедшее недавно обновление системы (Byzantium) является первой частью перехода на следующий этап развития платформы (Metropolis). Ожидается, что вторая часть обновления (т.н. Constantinople) выйдет в следующем году. Обновление должно **изменить способ майнинга криптовалюты**. Сейчас — это решение криптографических задач с затратой огромного количества электроэнергии. Планируется переход на алгоритм, который доверит богатым участникам системы с большой долей эфира подтверждать транзакции без традиционного майнинга.

Другое немаловажное изменение — это **реализация стандарта ERC20 в протоколе**. Сейчас стандарт ERC20 закреплен лишь на бумаге, токены могут значительно отличаться от описанного стандарта. Реализация ERC20 в протоколе Ethereum позволит формализовать проверку на программном уровне и исключить невалидные токены.

Мы **прогнозируем рост количества взломов веб-приложений блокчейн-проектов за счет фишинга**, самого простого и работающего способа атаки. Внимание злоумышленников также будет направлено на веб-кошельки (MetaMask, Mist) — они являются компромиссом для тех, кто не хочет хранить полную копию блокчейна у себя на компьютере, однако надо помнить, что кошелек в вебе — это хоть и удобно, но небезопасно, рано или поздно они будут взломаны. С другой стороны, мы ожидаем улучшения качества смарт-контрактов за счет развития инструментов, повышения осведомленности разработчиков в вопросах информационной безопасности, устранения ошибок в виртуальной машине Ethereum; развития более безопасных альтернатив Ethereum (например, HyperLedger), а также появления большого числа инструментов и программ для обычного пользователя.

Аппаратные атаки

В 2016 году мы затрагивали тему уязвимости «железа». В частности, обнаружили в процессорах Intel недокументированную лазейку, которая потенциально может позволить злоумышленнику включить отладочный интерфейс и фактически получить полный контроль над компьютером жертвы. Мы также прогнозировали, что это не последняя наша находка. И оказались правы.

В 2017 году мы продолжили исследовать платформу Intel: в частности, был **подробно изучен так называемый «тайный» процессор Intel ME**, чья функциональность для многих исследователей остается не до конца раскрытой. Intel Management Engine (Intel

[4] Токенсейл – продажа токенов.

ME) — это отдельный процессор, встроенный в чипсет материнской платы, со своей операционной системой MINIX. Он может работать даже тогда, когда компьютер выключен. Компания Intel проектировала этот процессор для удаленного облуживания и мониторинга ПК во время сна или работы.

Нам удалось найти уязвимость и использовать ее для активации аппаратной отладки (JTAG) для Intel Management Engine, которая позволяет получить полный доступ ко всем устройствам PCH (Platform Controller Hub), используя технологию Intel DCI (через интерфейс USB). Данный **недостаток в системе безопасности Intel открывает доступ потенциальным злоумышленникам во все компьютеры, ноутбуки, мобильные устройства, где есть процессор Intel Skylake и выше. А это — миллионы устройств по всему миру. Это может быть потенциально использовано злоумышленниками для расшифровки жесткого диска.**

С помощью Intel ME злоумышленник может получить доступ в том числе к изображению на экране, клавиатуре и мышке (вне зависимости от того, какая операционная система используется). При этом такой «захват» может происходить совершенно незаметно для средств защиты, установленных в операционной системе. Если в ME попадет зловредный код, то он может оказаться настолько «живуч», что даже полное форматирование диска и/или полная переустановка системы не окажут на него сколько-нибудь значимого влияния. Мы уведомили об этом Intel. Защиты пока не придумано.

Самая большая проблема, связанная с взломом этой технологии, состоит в том, что **может появиться новое поколение вирусов, которое не отслеживается современными средствами обеспечения безопасности** (антивирусы, файрволы), потому что они работают совсем в другом окружении. Фактически они работают не на основном процессоре, а на абсолютно другой микросхеме, которая, с одной стороны, имеет доступ ко всем данным, которые вы обрабатываете на компьютере, а с другой – ее невозможно контролировать.

Даже когда Intel выпустит обновления, связанные с безопасностью и устранением/закрытием этой ошибки обновления, останется возможным так называемый даунгрейд — обновление на более старую версию. И злоумышленник всегда может поставить уязвимую версию, в контексте этой уязвимости получить доступ к секретным данным вашей платформы, после чего откатить изменения. И вы даже не сможете понять, скомпрометирована ваша система или нет.

Исследователи проявляют интерес к этой технологии, так как она выводит на другой уровень таргетированные атаки, а также атаки криптолокеров[5], когда не просто блокируются ваши данные, но и выводится из строя материнская плата. И вернуть систему к жизни можно только с помощью дорогого ремонта, заменой микросхем, что в принципе равноценно покупке новой системы. Это может спровоцировать новый этап в развитии зловредного вымогательского ПО, которое позволяет за выкуп восстанавливать платформу к жизни. Пока мы не зафиксировали ни одного случая такого взлома, выполненного «плохими парнями». Тем не менее, как показывает опыт, это вопрос времени.

[5] Атака программы-вымогателя CryptoLocker — кибератака с использованием программы-вымогателя CryptoLocker, троянской программы, заражающей компьютеры под управлением операционной системы Microsoft Windows. При заражении компьютера вредоносная программа шифрует определённые типы файлов, хранящихся на локальных и подключённых сетевых дисках, используя криптосистему с открытым ключом RSA, причём закрытый ключ хранится только на серверах управления вредоносной программой. Затем вредоносное ПО отображает сообщение, которое предлагает расшифровать данные, если платеж (через биткойны или предоплаченный кассовый ваучер) производится в указанный срок, и пользователю будет угрожать удаление закрытого ключа в случае истечения срока.

Для заметок

Для заметок

Для заметок