POSITIVE TECHNOLOGIES

Кибербезопасность — 2018–2019: итоги и прогнозы

Содержание

Наше дело предупредить. Фантастические (и не очень) прогнозы Positive Technologies на 2019 год и итоги последних 12 месяцев.

Введение

Многие нашумевшие события в сфере информационной безопасности можно было предотвратить. На рубеже 2015–2016 годов аналитики крупнейших компаний в сфере кибербезопасности сообщали о растущей проблеме вирусов-вымогателей, а почувствовать ее в полной мере бизнесу пришлось в 2017 году. В 2013–2014 годах вошел в обиход термин APT (advanced persistent threat, то есть «целевая кибератака»). При этом мало кто понимал, что же такого опасного для бизнеса в этой фактически военной аббревиатуре, пока в 2016 году группировка Cobalt не начала серийно грабить банки.

Минувший год в глобальном плане стал относительно спокойным. Однако не стоит обманываться: новые проблемы накапливаются, число мелких и средних инцидентов растет, а киберпреступники активно изучают открывающиеся возможности. Говоря языком теории катастроф, некоторые точки бифуркации уже наметились. Представляем вашему вниманию итоги прошедшего года и прогнозы на 2019 год, сделанные практикующими исследователями и экспертами Positive Technologies.

Борис Симис,
заместитель
генерального директора
Positive Technologies

2018: общие тенденции ИБ

Цифровизация, aka Уязвимость

В основе масштабной и быстрой цифровизации всех сфер жизнедеятельности и бизнеса, которую мы сейчас наблюдаем, лежит использование массы информационных технологий (как уже апробированных и вызывающих доверие, так и новейших). Однако, как показывает практика, даже в уже использующихся годами технологиях вопросы безопасности не решены. Всеобщая безопасность спотыкается о грабли несоблюдения основ кибергигиены: в пугающем количестве аудитов мы сталкиваемся с необновленным ПО, с отсутствием культуры патч-менеджмента, с дырявым периметром. В сухом остатке мы имеем общий рост числа инцидентов (по нашей оценке, в этом году число инцидентов ежеквартально увеличивалось на треть). Не меньшую роль в условиях цифровизации общества и бизнеса играет сращивание и взаимопроникновение информационных технологий — веб-сервисов, телекоммуникационных систем, систем защиты, информационных систем и других (зачастую в рамках одного бизнес-процесса). На их стыках возникают так называемые слепые для узкоотраслевых экспертов зоны, открывающие киберпреступникам новые возможности для гибридных атак, то есть атак, использующих уязвимости самых различных технологий. Такие атаки были и раньше, но их было исключительно мало, сейчас число их увеличивается, так как технологии нападения идут вперед семимильными шагами, с успехом используя все нюансы цифровизации. Опыт показывает, что на практике в условиях цифровизации сосуществуют обе тенденции (иногда даже в рамках одной компании), сохраняя свою актуальность.

Изначальная нерешенность задач кибербезопасности на уровне IT благодаря стартовавшей в государстве идее цифровизации сейчас оперативно масштабируется на сферы жизнедеятельности и бизнеса, исторически не подготовленные к эффективному отражению кибератак: на сектора реальной экономики, интернет вещей, частную жизнь граждан и пр. В связи с этим бизнес неизбежно должен начать уделять больше внимания оценке реального положения дел в каждой отдельно взятой информационной системе и с большей точностью просчитывать варианты последствий. В свою очередь, это станет катализатором для развития технологий различного типа — от интеллектуального управления активами до расследования инцидентов с различным уровнем ретроспективы и адаптацией к уникальным инфраструктурам.

Динамика отечественного рынка ИБ

Итоги 2018 года показывают, что в общей сложности рынок ИБ в России вырос очень незначительно: общий прирост не превысит 10% по сравнению с показателями прошлого года. При этом позитивную динамику рынок получает за счет запуска отдельных проектов в области цифровизации федерального уровня (например, перевода городского хозяйства на новые технологии, появления умных городов, умного транспорта, государственных сервисов), а также за счет ряда крупнейших игроков отечественного рынка, выбравших для себя путь цифровой трансформации и понимающих необходимость некоей безопасности 2.0 — подхода, основанного не только на отражении атак, но и на проактивном выявлении угроз.

Одним из ключевых драйверов отечественного рынка продолжают оставаться деятельность регуляторов и государственные инициативы, направленные на повышение защиты критически важных инфраструктур. Под давлением регуляторов компании серьезно подойдут к безопасности, проведут категорирование и начнут более пристально вглядываться в собственную инфраструктуру. Это дает основания ожидать обнаружения старых целевых атак. Объекты КИИ обратят внимание на свою инфраструктуру и начнут выявлять у себя инциденты, увидят, что были атакованы какое-то время назад. В следующем году мы ожидаем новостей из мира большого бизнеса о такого рода взломах и атаках.

Алексей Новиков,
директор экспертного центра безопасности Positive Technologies

APT, шпионаж и фишинг

APT как новый старый тренд

С точки зрения массовых эпидемий прошедший год был спокойным, но в целом ситуация не улучшилась. Число уникальных киберинцидентов продолжает увеличиваться: по нашей статистике, средний прирост числа инцидентов за три квартала этого года составил 34%. Одна из причин — существенно снизившийся порог входа в киберпреступность: злоумышленнику уже не нужно обладать высоким уровнем знаний в области IT, достаточно купить готовые инструменты и инструкции в дарквебе. На рынке появляются универсальные трояны, которые можно использовать как для шпионажа и кражи данных, так и для удаленного управления устройствами, а спрос на разработку и распространение ВПО значительно превышает предложение. При этом использование криптовалюты для оплаты существенно упрощает куплю-продажу. К тому же наличие криптовалют как таковых обеспечило злоумышленников новым способом относительно легкой монетизации взломанных ресурсов: например, пять лет назад продажа доступа к 1000 взломанных ПК приносила злоумышленнику до 20 $, теперь же, имея доступ к этим же 1000 ПК, он может зарабатывать до 600 $ ежемесячно на майнинге криптовалюты. В нашей практике в этом году был опыт расследования инцидентов, в ходе которых злоумышленники получали нелегитимный доступ к серверам, используя уязвимости в phpMyAdmin, формировали ботнет и с его помощью майнили криптовалюту (в одном из случаев ботнет численностью около 5000 серверов обеспечивал злоумышленнику прибыль около 200 000 руб. в месяц). Это, конечно же, в первую очередь приводит к росту массовых атак в целом.

Что касается корпоративного рынка, то он все чаще оказывается жертвой APT. По итогам прошлого года мы отмечали, что так или иначе с целевыми атаками столкнулась практически каждая вторая организация. В этом году ситуация сохранилась. В силу ужесточающихся требований со стороны регуляторов в области обнаружения и предупреждения компьютерных атак все большее число компаний задается вопросом: «А не взломаны ли мы?». В половине случаев в нашей практике ответ на этот вопрос положительный. Ретроспективный анализ событий ИБ и работы по тестированию на проникновение выявляют векторы проникновения в инфраструктуру, следы того, что эти векторы уже были использованы, а также следы присутствия злоумышленника в инфраструктуре.

Проводимый нами анализ киберугроз в этом году показал, что целевые атаки впервые стали преобладать над массовыми, а их доля составила 54% и 55% во втором и третьем кварталах соответственно. И в ближайшее время компании все чаще будут сталкиваться именно с целевыми атаками: чем эффективнее выстраиваемая организациями защита, тем менее успешными являются массовые атаки на них, это неизбежно приведет к росту APT.

Шпион, выйди вон

Нельзя также сбрасывать со счетов и сложные длительные атаки на промышленные предприятия, целью которых чаще всего является промышленный шпионаж. В 2018 году в рамках расследований команда PT Expert Security Center обнаружила следы компрометации некоторых компаний из отрасли промышленности новой группировкой, названной экспертами TaskMasters[1]. Проведенный анализ показал, что первичное проникновение в инфраструктуру этих компаний произошло несколько лет назад (самые ранние случаи — 2010 год).

1 Группировка, выявленная экспертами PT Expert Security Center в 2018 году и использовавшая необычный метод закрепления в инфраструктуре, основанный на создании специфических заданий (тасков) в планировщике задач. Это и послужило поводом для названия TaskMasters.

Как правило, госкомпании становятся жертвами атак на веб-приложения с целью подмены страниц сайта (дефейса) или отказа в обслуживании, но не меньшее число атак направлено на хищение данных (планов стратегического развития, информации ограниченного доступа и т. п.). В течение года эксперты PT Expert Security Center зафиксировали на территории России и стран СНГ активность 12 различных APT-группировок, нацеленных именно на получение данных. При этом участились случаи использования фишинга, направленного на личные (не корпоративные) электронные адреса сотрудников и особенно топ-менеджмента компаний, для последующего развития атаки.

С большой долей вероятности атаки с целью кибершпионажа продолжатся и в 2019 году. При этом можно прогнозировать, что большинство из них станут всего лишь продолжением ранее успешно выполненных проникновений.

Бессмертный Cobalt & Co.

По данным ФинЦЕРТ, ущерб банков от кибератак в 2018 году значительно снизился по сравнению с прошлым годом (с более чем 1 млрд рублей до 76,5 млн). Это может быть связано с арестом лидера группировки Cobalt. Тем не менее атаки не прекратились: в течение этого года рассылки от Cobalt (или ее части) фиксировались экспертами PT Expert Security Center в общей сложности более 50 раз. Группировка несколько раз в течение года меняла свой инструментарий: сначала это был Beacon Cobalt Strike, в середине года — JS-backdoor, а к концу года — CobInt. В течение года несколько раз поменялась тактика доставки вредоносных вложений: вредоносный документ, архив с паролем, ссылка на вредоносный документ в теле письма, вложение в виде PDF-файла. В своих вредоносных документах они используют свежие эксплойты (например, в одной из декабрьских рассылок была использована уязвимость нулевого дня — в течение нескольких часов после ее появления), используют новые методы атак и инструменты, адаптируя их для своих нужд за считанные часы. География атак в этом году была обширной: Россия и СНГ, Болгария, Боливия, Великобритания, Вьетнам, Германия, Италия, Кипр, Польша, Румыния, Сербия, Турция, Филиппины, Эстония, ЮАР и другие страны.

Помимо этого, на протяжении года на территории России и стран СНГ проявляла активность группировка Silence, которая также специализируется на атаках на финансовый сектор. В общей сложности было зафиксировано пять их атак (интенсивность совпадает с прошлогодней). Появилась и новая группировка: используемый инструментарий, методы атак и ряд других артефактов не позволяют соотнести ее с одной из уже известных. За период с октября по декабрь были зафиксированы две рассылки.

Хотя успешных крупных хищений на территории России в этом году не было, однако общая активность группировок позволяет прогнозировать возможное увеличение фиксируемого ФинЦЕРТ ущерба в 2019 году.

Киберпреступник — кто он?

Сегодня грань между преступностью и киберпреступностью практически стерта: провести хакерскую атаку может едва ли не каждый. Тем не менее нынешний киберпреступник — это в большинстве случаев группировка; одиночек, организующих атаку самостоятельно от начала и до конца, нет. Атаки стали сложнее, и злоумышленникам необходимо кооперироваться. И даже если троян в дарквебе покупает кто-то один, очевидно, что такой человек не пишет вредоносное ПО сам, а покупает криптор и уже с приобретенным пакетом проводит атаку. То есть даже в этом случае у него есть подельники. Успешный хакер сегодня — это хороший управленец, который набрал команду, а сам, возможно, вообще не является программистом. Это значительно затрудняет атрибуцию атак при их расследовании, а также увеличивает общее число вовлеченных в киберкриминальную деятельность субъектов.

Старый добрый фишинг

По-прежнему основными методами проникновения в инфраструктуру компаний, в том числе банков, остаются фишинг и использование вредоносного ПО: в 61% атак на банки в первой половине 2018 года мы видели эти методы. Так действуют, например, упомянутые выше группы Cobalt и Silence. Наиболее вероятная мишень преступников в этом случае — банки среднего звена, у которых можно украсть достаточно большие суммы денег и которые не готовы вкладывать сверхбюджеты в обеспечение собственной безопасности. Небольшие банки могут оказаться промежуточным звеном атаки: например, с компьютеров их сотрудников могут рассылаться фишинговые письма в адрес их коллег из более крупных банков. В тренде у преступников использование уязвимостей в продуктах Microsoft, причем все чаще используются вновь опубликованные эксплойты (окно между появлением новой технологии и принятием ее на вооружение может исчисляться часами). Более того, стоит ожидать, что преступники будут вкладывать значительные средства в закупку неопубликованных эксплойтов для уязвимостей нулевого дня на теневом рынке.

Дмитрий Скляров,
руководитель отдела анализа приложений Positive Technologies

Процессорные уязвимости

Стадии развития технологий в современном мире весьма последовательны: от возникновения идеи, которая может дать какую-то выгоду, разработки концепции заработка на ней, реализации ее бизнесом, до востребованности пользователями — и заинтересованности в ней злоумышленников, желающих обогатиться. В этот момент бизнес начинает привлекать ИБ для обеспечения работоспособности системы в случае кибератак таким образом, чтобы при этом не страдали ее пользователи. При этом сама такая идея может изначально оказаться в эксплуатации не у конечного пользователя (не обладающего достаточными ресурсами для обеспечения безопасности), а у другого бизнеса, которому есть что терять, и он готов превентивно заплатить за снижение рисков. Бывают, однако, случаи, когда исследователи начинают действовать по собственной инициативе (почти так получилось с Intel Management Engine).

Сколько еще будет уязвимостей в процессорах

При разработке концепций современных процессоров ключевой целью были вычислительные мощности и быстродействие. Однако оптимизация в погоне за скоростью подарила нам впоследствии уязвимости Meltdown и Spectre. Безусловно, уязвимости в процессорах ведущих производителей — один из основных трендов 2018 года, и есть все основания ожидать в будущем продолжения истории, которая пока только началась. При этом сложно прогнозировать, когда она закончится, потому что общее число специалистов по ИБ, которые в полной мере понимают, как работают современные процессоры, мало: архитектура CPU не документирована, и уязвимости находят по крупицам. Скорее всего, проблем безопасности в процессорах гораздо больше, и исследователям нужно просто задаться целью их поиска. Не последнюю роль в развитии темы играют и максимальные в истории программ bug bounty выплаты со стороны Intel: за выявленную уязвимость уровня Meltdown исследователь может получить до 250 тысяч долларов. Последствия ошибок в CPU могут иметь отложенный эффект: более пяти лет назад исследователи предупреждали о том, что гипотетический злоумышленник может спрятать вредоносный код во флеш-памяти, и даже обновление ПО не поможет от него избавиться. А первый массовый случай использования такой атаки был зафиксирован только в этом году. По аналогичному сценарию может развиваться история обнаруженной нами уязвимости в Intel Management Engine: злоумышленники начнут ее использовать, как только научатся это делать.

Когда уязвимости в CPU начнут использовать

Пока исследователи на шаг впереди атакующих: мир еще не сталкивался с эксплуатацией процессорных уязвимостей. В частности, использования Meltdown мы пока не видели, скорее всего, потому, что пока нет эффективного (в сравнении с уже используемыми) способа монетизации этой уязвимости. Наши исследования показывают, что именно финансовая выгода является одним из ключевых мотивов для атакующих. Это актуально и в истории с Intel ME: слишком сложно что-то делать с флеш-памятью, прошивками и чипсетами, тогда как банальный фишинг позволяет получить большую отдачу при меньших вложениях; социальная инженерия значительно проще позволяет выполнить успешную атаку: в среднем 27% сотрудников склонны переходить по ссылкам из фишинговых писем. Таким образом, неиспользование атакующими процессорных уязвимостей в массовых (тиражируемых) атаках связано с экономией ресурсов. С другой стороны, есть области, в которых меры безопасности реализованы максимально жестко (к примеру, это характерно для некоторых научно-исследовательских, оборонных, промышленных объектов), поэтому эксплойты под процессорные уязвимости могут создаваться продвинутыми кибергруппировками в рамках целевых атак уже сейчас. Но такие атаки вряд ли будут массовыми. Спровоцировать массовость использования уязвимостей в CPU может либо появление нового способа их эффективной монетизации — либо очередная утечка готового инструментария, как было в случае с EternalBlue.

Привет из прошлого

Сегодня в мире существует множество так называемых end-of-life-устройств, производство которых завершено, вендор прекратил выпуск обновлений ПО, а значит, и уязвимости в них никогда не будут закрыты. Стоит вспомнить хотя бы пресловутый Windows XP, который уже не поддерживается производителем, но все еще используется. Однако если для Microsoft стандартная практика — объявлять о дате прекращении поддержки своего ПО за несколько лет и требовать от пользователей регулярного обновления ПО, то в аппаратных решениях такого не наблюдается. Например, большинство домашних роутеров не обновляются ни разу за весь срок работы, и прямой коммуникации между производителем и пользователем обычно не предусмотрено. Ситуация усугубляется еще и скоростью обновления линеек устройств и, соответственно, снятием с поддержки устаревшего оборудования. Если поддержка роутера прекращена производителем и устройство не поддерживает прошивки энтузиастов, такие как OpenWrt, то единственная возможность избавиться от таких уязвимостей — сменить оборудование. Но даже когда исследовали информируют вендора о проблеме, оповещения для пользователей публикуются очень неохотно. В следующем году может продолжиться массовая эксплуатация старых аппаратных уязвимостей, о которых уже известно, но пока нет ПО для их использования.

Число устройств, поддержка которых окончена, растет с каждым годом. Злоумышленники начинают атаковать их все чаще. Если несколько лет назад ошибки в роутерах практически не эксплуатировали, то с появлением ботнетов-миллионников роутеры для хакеров стали популярными и монетизируемыми устройствами. Нельзя забывать и о том, что, получив контроль над роутером, злоумышленник может успешно атаковать все, что «за ним», — ПК и IoT-устройства.

Владимир Назаров,
руководитель отдела безопасности промышленных систем Positive Technologies

Рискованная промышленность

Количество уязвимостей в АСУ ТП по-прежнему растет

В 2018 году сохранилась динамика прошлого года: число опубликованных в 2017 году уязвимостей на 71% выше аналогичного показателя 2016 года, показатели 2018 года по состоянию на сегодняшний день превышают прошлогодние еще на 10%. Только за прошедший год с помощью экспертов Positive Technologies было выявлено и устранено около 30 уязвимостей, еще чуть более сотни отправлены вендорам и ожидают соответствующих патчей. Более половины выявленных в течение года уязвимостей оцениваются экспертами Positive Technologies как уязвимости высокой степени риска. Их использование может позволить гипотетическому злоумышленнику влиять на работоспособность АСУ ТП вплоть до возникновения аварий. В целом результаты наших работ по анализу индустриального оборудования говорят о том, что вендоры далеки от безопасной разработки by design, а количество находимых уязвимостей не снизится и в следующем году. Например, в оборудовании и SCADA-системе одного из исследованных вендоров в этом году обнаружено более 50 уязвимостей нулевого дня.

Разработка и применение кибероружия продолжатся

В этом году были обнародованы детали атаки с использованием кибероружия Triton, очередного вредоносного ПО, которое заточено под специфическое оборудование Schneider Electric. А последующая публикация части исходников этого ПО в интернете вкупе с доступностью таких поисковиков, как Shodan, создают предпосылки для повтора таких атак гипотетическим злоумышленником, причем высокой квалификации от него уже не требуется. Мы прогнозируем, что в 2019 году будут продолжаться разработка и использование кибероружия, направленного на конкретные модели промышленных устройств и закрытые протоколы. То есть история, начавшаяся со Stuxnet и Industroyer, получит продолжение.

Нецелевые атаки на промышленные предприятия

В 2018 году произошло несколько довольно громких инцидентов в промышленных компаниях, в частности Boeing заявил об атаке WannaCry, а спустя несколько месяцев тот же вирус стал причиной приостановки заводов Taiwan Semiconductor Manufacturing Company. Атаки были нацелены именно на IT-инфраструктуру, а не на само промышленное оборудование. Однако воздействие на нее (например, на рабочие станции или сетевое оборудование) может негативно повлиять на штатное функционирование промышленных систем. Например, в конце ноября 2018 года из-за вируса-шифровальщика была парализована работа только что открывшейся канатной дороги на Воробьевых горах в Москве.

Сохранение такой тенденции прогнозируется и в 2019 году.

Криптовалюты вместо чистой воды

Популярность криптовалют спровоцировала интерес киберпреступников к майнингу, для которого использовались в течение этого года различные ресурсы. Около четверти всех атак с использованием вредоносного ПО в первом квартале 2018 года выполнялись с целью распространения майнеров криптовалюты, а к началу четвертого квартала их доля снизилась до 20%. Некоторая доля таких атак пришлась и на оборудование промышленных предприятий. Например, в феврале на серверах некоторых европейских водоочистительных сооружений был обнаружен майнер криптовалюты Monero. Его опасность в том, что из-за его работы быстродействие SCADA-системы падает ниже требуемого уровня, что потенциально может привести к аварии. Однако падение курса криптовалют, скорее всего, приведет к тому, что общее число атак с целью майнинга в ближайший год пропорционально снизится.

Закон добрался до интернета вещей

В течение всего 2018 года продолжился рост числа скомпрометированных устройств интернета вещей. Проблема защищенности IoT вышла на государственный уровень: власти Великобритании выпустили руководство по обеспечению защиты IoT от распространенных кибератак, а в штате Калифорния вышел закон, обязывающий производителей устройств, подключаемых к интернету, обеспечивать дополнительные меры защиты, предотвращающие возможность несанкционированного доступа, модификации или утечки данных. Тем не менее в 2019 году прогнозируется продолжение роста скомпрометированных IoT-устройств ввиду традиционно низкого уровня их защищенности. Актуальность сохраняет и проблема использования IoT-устройств со стандартными паролями или с незакрытыми уязвимостями.

Деньги под прицелом

Ярослав Бабин,
руководитель группы исследований безопасности банковских систем Positive Technologies

Финансовая выгода теряет позиции

Финансовые организации продолжают входить в тройку наиболее популярных среди киберпреступников объектов атак. Ключевыми мотивами кибератак этого года стали прямая финансовая выгода, а также получение данных, в том числе учетных данных для доступа к финансовым приложениям и данных банковских карт. Одним из вариантов их последующей монетизации является перепродажа на теневом рынке: около 80% всей продаваемой в дарквебе информации это всевозможные «учетки» и данные банковских карт. При этом данные для доступа к личным кабинетам в онлайн-банках продаются поштучно. При средней цене в 22 $ такие счета имеют баланс от нескольких десятков долларов до нескольких тысяч. Средняя стоимость данных одной банковской карты с балансом от нескольких сотен долларов составляет всего 9 $. Данные банковских карт в дальнейшем могут быть использованы для покупки товаров в интернете или изготовления дубликатов банковских карт для снятия наличных в банкоматах.

Уязвимые банкоматы

В числе трендов года также стоит отметить распространение готового ВПО для опустошения банкоматов. На теневом рынке сегодня можно купить не только сам инструмент и инструкцию по эксплуатации, но и техническую поддержку. Стоимость такого ВПО достаточно высока и начинается от 1500 $. Однако потенциальная прибыль значительно превышает расходы: ВПО может окупиться уже после одного успешного ограбления, при этом разработчики стремятся адаптировать программы для как можно большего числа моделей банкоматов. Резонансной новостью стало появление в конце 2017 года ВПО CutletMaker, которое было оценено в дарквебе в сумму порядка 5000 $ и продавалось вместе с подробной инструкцией. При этом общая защищенность банкоматов от логических атак оставляет желать лучшего: в январе 2018 года Секретная служба США, а также крупнейшие производители банкоматов Diebold Nixdorf и NCR выпустили экстренные предупреждения, в которых сообщалось об угрозе атак на банкоматы. Собственные исследования Positive Technologies в этом году продемонстрировали высокий процент устройств, уязвимых для атак типа Black Box (до 69% банкоматов), атак на сетевом уровне (до 85%), атак, связанных с отсутствием шифрования жесткого диска (до 92%), для выхода из режима киоска (76%). Перехват данных банковских карт оказался возможным на всех исследованных устройствах, а в 88% случаев исследователям удавалось обойти установленные на банкоматах решения класса Application Control, в том числе из-за уязвимостей нулевого дня в коде самих средств защиты.

Black-трейдинг

Исследования 2018 года продемонстрировали и недостаточную защищенность торговых терминалов, позволяющих покупать и продавать акции, облигации, фьючерсы, валюту и другие активы. В 61% случаев злоумышленник может получить возможность торговать активами пользователя приложения, получить информацию о доступных средствах на балансе, подменить параметры автоматической торговли, просмотреть историю и запланированные операции. Шестая часть обследованных приложений (17%) позволяет подменять отображаемые котировки за определенные периоды. Каждое третье приложение позволяет посторонним лицам осуществлять сделки по продаже или покупке акций от имени пользователя и без доступа к личному кабинету. Злоумышленник может увеличить стоимость интересующих его ценных бумаг с помощью массовой покупки их на чужих аккаунтах или снизить стоимость акций, активно продавая их. Аналогичным образом можно манипулировать курсами валют, если атака затронет крупных игроков или большое количество пользователей. При этом атаки на веб-версии торговых терминалов могут носить массовый характер: злоумышленник может внедрить скрипт в веб-приложение или разместить на другом популярном сайте вредоносную ссылку, тогда от лица любого пользователя, который зайдет в приложение или перейдет по ссылке, выполнится нелегитимная операция. В силу слабой защищенности трейдинговых приложений и традиционного стремления злоумышленников к легкой масштабируемости и быстрой монетизации атаки на пользователей трейдинговых систем имеют все шансы превратиться в массовые в ближайшие год-полтора.

Павел Новиков,
руководитель группы исследований безопасности телекоммуникационных систем Positive Technologiess

Телекомы в НЕбезопасности

Уязвимые сети

Операторы мобильной связи понимают важность обеспечения безопасности и предпринимают активные действия по нейтрализации основных угроз в отношении собственных систем и абонентов. В итоге удается снизить вероятность получения информации об абонентах и сети оператора. Тем не менее на сегодняшний день остается существенным риск проведения мошеннических операций: уязвимы 78% сетей. А перехват SMS возможен в 9 из 10 случаев. При этом в дарквебе, например, можно купить подписку на получение и подделку чужих SMS в реальном времени всего за 20 $ в месяц. По-прежнему существуют архитектурные особенности сигнальных сетей, которые не позволяют обеспечить полную защиту абонентов и операторов с помощью технических мер. Уязвимыми являются не только сети предыдущих поколений, но и активно применяемая сегодня технология 4G. Одним из ключевых приоритетов в защите телеком-сетей на сегодняшний момент является доступность сервисов (защита от DoS-атак), поскольку сеть должна работать всегда, а отсутствие связи — это очень серьезная угроза для производства, финансового сектора, энергетики, простых граждан и целого государства.

Подключенный мир

В ближайшие пару лет не стоит ожидать существенного улучшения ситуации в обеспечении безопасности мобильных сетей. В первую очередь, это потребует пересмотра современных стандартов и технологий работы сигнальных сетей. Сегодня все говорят о скором появлении сетей нового поколения (5G). Однако 5G создается не для обеспечения коммуникации и высокоскоростного мобильного интернета: с этими функциями успешно справляется нынешний LTE. 5G нужен для построения так называемого подключенного мира (internet of everything), где уже все будет связано со всем. Разработка стандарта мобильной связи пятого поколения все еще ведется, туда пытаются внедрить безопасность на уровне архитектуры, например путем добавления специального элемента безопасности

SEPP на границе сети. Однако риск проведения атак на сигнальные сети с целью перехвата пользовательского трафика (например, одноразовых паролей для подтверждения банковских транзакций) остается актуальным, особенно в первое время, когда сеть 5G будет работать «поверх» 4G-сети.

Немного о персональных данных

Отдельное влияние на обработку персональных данных и осознание их значимости оказывает General Data Protection Regulation (GDPR, общий регламент по защите данных), заставляющий всех игроков рынка (не только в Европейском Союзе) по-новому посмотреть на вопрос обработки и хранения такой информации. Тенденция такова, что все больше и больше компаний в мире (особенно это касается информационных гигантов, обрабатывающих большие массивы персональных данных), вне Евросоюза, распространяют на себя действие этого закона. С момента вступления его в силу 25 мая 2018 года прошло еще не так много времени, и многие компании, в том числе и европейские, еще не до конца понимают, как применять его нормы. В следующем году будет больше практики, больше прецедентов, больше решений надзорных органов, что приведет к лучшему пониманию и осознанию необходимости внедрения норм GDPR в бизнес-процессы компаний, в том числе и российских, если они хотят работать на европейском рынке. Косвенно GDPR уже начинает влиять и на персональные данные российских физических лиц, находящихся на территории России, — в дополнение к закону № 152-ФЗ «О персональных данных». Скорее всего, мы придем к необходимости изменения российского законодательства в сторону гармонизации с GDPR. Лишним подтверждением тому является подписание Российской Федерацией 10 октября этого года протокола о внесении изменений в Конвенцию Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» для приведения конвенции к реалиям сегодняшнего дня, а значит — и в соответствие с GDPR.

Николай Анисеня,
руководитель группы исследований безопасности мобильных приложений Positive Technologies

Мобильные угрозы

Переход на личности

Атаки на частных лиц оставались в тренде в 2018 году, и примерно пятая их часть происходит через мобильные устройства. Самым популярным способом атак все еще остаются вредоносные приложения, которые пользователь чаще всего устанавливает по невнимательности самостоятельно. Самым распространенным типом вредоносного ПО стали шпионские трояны, которые воруют информацию с устройств, в том числе пользовательский ввод и снимки экрана. Безусловно, атаки на частных лиц с использованием троянов, заражающих мобильные устройства и компьютеры жертв, продолжатся. Магазины приложений (Google Play и App Store) все строже проверяют приложения на наличие уже известного вредоносного ПО, поэтому можно ожидать появления новых его модификаций, не детектируемых средствами проверки. При этом осведомленность простых пользователей в вопросах ИБ по-прежнему остается на низком уровне, поэтому количество жертв таких атак не будет, скорее всего, снижаться в ближайшие 2–3 года.

Новые возможности — новые атаки

Мобильные устройства все сильнее интегрируются в рабочие процессы и в личную жизнь, и это неизбежно ведет к росту так называемой поверхности атаки — к расширению возможных способов вредоносного взаимодействия с мобильными устройствами и мобильными приложениями. Например, атаки через интерфейс для подключения к зарядке или к ПК находят новые применения. Под ударом оказываются не сами устройства и операционные системы (например, с целью повышения привилегий, root, jailbreak), а пользователи с их приватными данными, аккаунтами

в различных сервисах. Нашумевшая уязвимость в Bluetooth — Blueborne — коснулась по большей части мобильных устройств. Она позволяет получить полный контроль над устройством под управлением iOS или Android в радиусе действия Bluetooth. Помимо этого, сами мобильные операционные системы активно развиваются, предлагая разработчикам новые возможности для создания мобильных приложений с более сложной функциональностью. Приложения получают возможность теснее взаимодействовать друг с другом внутри устройства, отправлять и принимать данные от носимой электроники или от других устройств (элементов умного дома, автомобиля, платежных терминалов).

Защита не спит

Рост функциональных возможностей неизбежно создает плодородную почву для возникновения новых уязвимостей. В подобных условиях предугадать, откуда ждать следующего удара, практически невозможно. Но общий тренд таков, что мобильные трояны (банкеры, вымогатели, шпионы, adware и пр.) сохранят, скорее всего, свою популярность как одно из самых эффективных средств атаки на мобильные устройства и их пользователей.

Тем не менее разработчики мобильных ОС стараются как можно скорее устранять критически опасные уязвимости по мере их обнаружения и увеличивать скорость доставки обновлений на устройства. Растет число компаний, которые на регулярной основе проверяют защищенность своих мобильных приложений. О безопасности задумывается не только финансовый сектор, непосредственно имеющий дело с деньгами, но и разработчики различных сервисов (такси, криптокошельки, соцсети, игры). Такая позитивная тенденция в стремлении повысить безопасность сервисов сохранится, мы надеемся, и в будущем.

Заключение

Иногда кажется, что исследователи информационной безопасности ведут себя чересчур беспокойно, сгущают краски. Это означает лишь одно: они знают то, чего не знают и не видят простые люди.

Сегодня мы наблюдаем опасную концентрацию проблем практически во всех сферах. Главная опасность нас ждет, если хакеры научатся эксплуатировать процессорные уязвимости. Спусковым крючком может стать утечка готового инструментария спецслужб, как было в случае с EternalBlue.

Теряет актуальность тема криптовалют, но защита торговых терминалов на биржах ценных бумаг оказывается не лучше, чем у криптокошельков, что чревато атаками на курсы валют и акций.

Переход нефтегазовой отрасли на интеллектуальные месторождения, работающие по сути на автопилоте, оказывается столь быстрым, что сценарий, при котором злоумышленники останавливают нефтедобычу по всему миру, при таком количестве уязвимостей в АСУ ТП уже не кажется фантастическим.

В телекоме уязвимы 78% сетей, но SMS-сообщения — все еще безальтернативный способ двухфакторной аутентификации. При этом широко внедряются новые, «недообследованные» технологии, такие как удаленная биометрическая идентификация, а уровень осведомленности населения о проблемах ИБ по прежнему остается невысоким.

Проблем, как вы видите, много, и задача специалистов по информационной безопасности, разработчиков ПО и государства — сделать так, чтобы негативные сценарии никогда не воплотились в жизнь.

Cybersecurity 2018-2019_A4.RUS.0002.02.DEC.18.2018