—Ого, какая ИБ!

ОСОБО ГОРЯЧИЕ ОБСТОЯТЕЛЬСТВА ИЗ МИРА КИБЕР-БЕЗОПАСНОСТИ. ИТОГИ 2022-ГО И ПРОГНОЗЫ НА 2023 ГОД ПО ВЕРСИИ POSITIVE TECHNOLOGIES

ptsecurity.com

Содержание

Технологические тренды в России и мире: разработка масштабных продуктов с нуля и доверие к облакам 3

Рынок кибербезопасности: общие тренды 6

- Рынок информационной безопасности в России: рост вопреки прогнозам 6
- Главные итоги и тренды законотворчества в сфере ИБ 7
- Смена парадигмы ИБ, переход к результативной защите и что еще принесет 2023 год 9

Кто и как атакует российские организации 12

- Уязвимости ради безопасности 15

Самые громкие атаки и самые атакуемые отрасли 17

- Государственные организации — цель №1 18
- Медицина лидирует по утечкам данных 19
- Промышленный сектор: нацеленность на остановку технологических процессов 20
- Финансовый сектор: наилучшая подготовленность к атакам, но в целом уровень защиты недостаточный 23
- IT-компании: осторожность в использовании открытого ПО и контроль цепочек поставок 25
- Наука и образование страдают от шифровальщиков 26

Атаки на пользователей: 2022 год запомнился масштабными утечками данных 26

Безопасность операционных систем: обзор тенденций и прогнозы на 2023 год 28

Безопасность мобильных приложений и устройств: брешей становится меньше, а специалистов по анализу защищенности по-прежнему не хватает 29

Искусственный интеллект и безопасность: чем запомнился 2022 год и чего ждать в 2023-м 31

Крипта, блокчейн, метавселенные и не только 33

Заключение 37

Технологические тренды в России и мире:
разработка масштабных продуктов с нуля и доверие к облакам

Алексей Андреев, управляющий директор
Positive Technologies

Алексей Астахов, руководитель продуктов
Application Security, Positive Technologies

Технологические тренды в ИБ и факторы, которые будут формировать тенденции в 2023 году:

Переход на отечественное ПО

В России ярко проявился вектор перехода компаний на отечественные операционные системы (ОС), что прямо повлияло на поддержку российских ОС вендорами ИБ. Так, большая часть продуктов Positive Technologies еще в 2022 году начала поддерживать ОС Astra Linux, в 2023 году мы продолжим развитие в этом направлении, а также будем добавлять и другие отечественные ОС.

Острая необходимость в практической ИБ

Запрос на практическую кибербезопасность стоит ребром как никогда, и это прямо определяет запрос к российским вендорам на качественные и практически применимые технологии в области ИБ.

Проблемы с железом

Недостаток железа в нужном объеме, а также нестандартных экземпляров — еще одна реалия 2022-го, с которой мы будем жить и в 2023 году. С одной стороны, эта ситуация подстегивает переезд в облака, а с другой — создает тренд большей фокусировки на софте и меньшей «заточки» под специализированное железо. Большой объем и легкая доступность железа позволяет более эффективно решать специфичные задачи. Сейчас важно, чтобы софт работал максимально универсально на типовых конфигурациях и в облачных средах, и приходится мириться с появляющимся оверхедом за счет универсализации.

Непрекращающиеся атаки на критическую инфраструктуру

Общая динамика роста атак заставляет пересмотреть и взгляды разработчиков средств защиты: любая защищаемая сущность (будь то инфраструктура, ее элемент или приложение) будет постоянно находиться под атаками. А это означает, что речь идет о другом профиле нагрузки, который нужно учитывать на самых ранних этапах разработки продуктов, — при их проектировании, наполнении знаниями и нагрузочном тестировании.

Разработка отсутствующих в России продуктов ИБ с нуля

Одно из главных последствий нестабильного года на рынке ИБ — это уход западных вендоров. Если рассуждать поверхностно, то российские вендоры выиграли с точки зрения конкуренции. Однако, если смотреть глубже, то становится очевидно, что это колоссальная потеря тех компонентов и модулей, из которых создавались продукты — нет западных облаков, привычных managed services и систем для разработки. Мы оказались в ситуации, когда мы либо создаем свои компоненты, либо пользуемся доступными, но менее качественными.

При этом, как за очень короткий срок разработать такие системы, которые на западе делались десятилетиями, менялись в результате конкуренции, эволюционировали? Например, NGFW. Задача разработать эффективный NGFW — это вызов. Качественный файрвол на должном уровне разработали всего три компании в мире, и все они не российские. Это технологически сложный продукт с высокими требованиями к качеству (отказоустойчивости, нагрузкам). Чтобы нам преодолеть этот разрыв с Западом, нужно найти уникальный путь. И часто в том пути, который западные компании шли десятилетиями, есть объективные причины, чтобы его не повторять.

Конечно, есть вещи, которые нельзя поменять, имея уже сложившийся рынок. Например, невозможно сделать новую сетевую «железку», не повторив все те протоколы, которые все еще встречаются в интернете. Но если смотреть на причины, по которым до сих пор существуют почти все сетевые технологии, созданные начиная с 60-х годов, — это обратная совместимость. Устаревшие технологии, которые априори небезопасные, но их нельзя убрать в процессе эволюции. А в результате революции — можно. То есть тут тоже пространство для сокращения времени разработки и кратное улучшение технологической базы сетей.

Наконец, люди, те, кто имеет опыт создания подобных продуктов. Если проанализировать сколько времени в разработке специализированных продуктов тратится на получение опыта, то становится понятно, что до 85% времени команды без специализированного опыта уходит на получение этого самого специализированного опыта. Все эти факторы показывают, что ближайший год будет стартом для разработки новых технологических решений, которые раньше казались слишком масштабными.

Общемировые тренды, которые актуальны и в России

Безопасность становится аспектом качества продуктов и систем

Мы наблюдаем огромный интерес к ИБ и безопасной разработке со стороны именно разработки и всех ролей, участвующих в создании продуктов. Несколько лет назад, когда кибератаки были менее активными, вся безопасность сводилась к формальным соблюдениям правил и получении сертификатов. В текущем моменте безопасность становится такой же гранью качества, как и возможность выдерживать повышенные нагрузки или иметь устойчивость к нетипичным условиям использования. Это означает, что важно создавать максимально удобные способы обеспечения безопасности для всех ролей, в тех форматах, в которых люди привыкли работать.

Для разработчиков — это IDE[1], для тестировщиков — фреймворки для тестирования, системы агрегации последовательности действий, для DevOps — CI/CD. Безопасность помогает каждой роли разработки быть более успешной в повседневной работе.

Более активное использование public, private облаков и контейнерных сред

С одной стороны, это общемировой тренд — он нацелен на более эффективное использование ресурсов, гранулярное управление сервисами, быстрый выпуск продуктов. С другой, в условиях дефицита железа, российские компании вынуждены ускорить этот переход. Мы видим, как сейчас даже самые консервативные организации переводят в контейнеры 1-2-3% своей инфраструктуры. Компании покупают и внедряют решения для частных облаков. Для разработчика средств защиты это означает что:

- все наши продукты должны быть готовы к тому, чтобы функционировать в этих средах;
- сами по себе контейнерные инфраструктуры тоже уязвимы и нуждаются в защите.

Настоящая экосистемность

Тренд на создание экосистем общемировой и не привязан к какой-то отдельной нише (ИТ, ИБ или какой-то еще). Если пользователь за счет объединения набора сервисов может получить более существенную ценность, то это и есть польза от экосистемы. С точки зрения ИБ, глобально есть два направления для создания экосистем: для защиты приложений и инфраструктурная. Если пользователи инфраструктурной экосистемы — это узкие специалисты по ИБ с большим опытом работы, предпочитающие работать в высокотехнологичных компаниях, то для экосистемы защиты приложений пользователи — это те самые люди, которые участвуют в создании продукта. Для инфраструктурной безопасности важно создать некий аналог автопилота, системы, которая сама отражает атаки, позволяет тратить минимум усилий на защиту и снижать требования к уровню тех, кто работает с системой. А для защиты приложений такой подход совершенно не будет работать: специалистов, создающих продукты, много, они технически подкованы, любят разбираться в мелочах и глубоко погружаться в предмет. Важно, чтобы, используя продукты, входящие в экосистему, такой специалист получал аккумулятивно больший эффект. Это вызов не только по части технической разработки продуктов, но и исследования и формирования способов взаимодействия с экосистемой в зависимости от роли пользователя.

[1] Программное приложение, которое помогает программистам эффективно разрабатывать программный код

Рынок кибербезопасности: общие тренды

Рынок информационной безопасности в России: рост вопреки прогнозам

Максим Филиппов, директор по развитию бизнеса
Positive Technologies в России

Ключевой фактор, повлиявший на конъюнктуру рынка кибербезопасности в России в 2022 году, — беспрецедентное количество хакерских атак на отечественные компании самых разных сфер бизнеса и активная позиция регуляторов и государства, переводящая практическую, результативную кибербезопасность в число ключевых потребностей. Вторая история, которая качественно изменила рынок: быстрый и массовый уход с рынка зарубежных производителей средств защиты информации.

Несмотря на то, что прогнозы аналитиков были скорее отрицательными (ожидалось сокращение объема рынка на 11%, а под объемом рынка в данном случае подразумевается объем денег, выплаченных клиентом)[1], по предварительной экспертной оценке Positive Technologies, рынок информационной безопасности в России за этот год вырос на 10-20%[2].

Массовые атаки, под которыми оказалась инфраструктура российских компаний, нашли отражение в существенном росте доли услуг в области кибербезопасности (работ, связанных с анализом защищенности, мониторингом событий информационной безопасности, реагированием на инциденты и их расследованием). В частности, объем подобных работ в Positive Technologies за 2022 год вырос больше чем в два раза.

Одним из наиболее востребованных рынком в 2022 году направлений стала Application Security, что и не удивительно с учетом специфики и количества атак на веб-приложения и информационные системы компаний в течение года. В частности, межсетевой экран уровня приложений (PT Application Firewall) и анализатор защищенности (PT Application Inspector) от Positive Technologies продемонстрировали более чем трехкратный рост в объеме продаж компании по итогам года, а динамический анализатор приложений (PT BlackBox), появившийся на рынке в третьем квартале 2022 года, к концу года насчитывает уже с десяток внедрений. Также, коммерческий успех в этом году получил новый продукт Positive Technologies — PT Extended Detection and Response (PT XDR), чей коммерческий релиз состоялся во втором квартале 2022 года. За неполный год выполнено 10 внедрений (самая масштабная инсталляция выполнена в инфраструктуре с более чем на 20 000 активов) и проведено более 50 успешных пилотных проектов, запланированных к реализации в первой половине 2023 года.

Наиболее эффективным и даже обязательным инструментом для обнаружения присутствия хакера в инфраструктуре стала система выявления атак в сетевом трафике — PT Network Attack Discovery — рост объема продаж в 2,5 раза. Де-факто ставшая стандартом индустрии линейка MaxPatrol продемонстрировала не менее впечатляющую динамику: число инсталляций MaxPatrol SIEM (системы выявления инцидентов ИБ в реальном времени) и MaxPatrol VM (системы нового поколения для управления уязвимостями) в 2022 году превысило 600 и 350 соответственно.

[1] По данным исследования Центра стратегических разработок (ЦСР)
«Прогноз развития рынка решений для информационной безопасности в Российской Федерации в 2022–2026 годах», август 2022 года.
[2] Собственная оценка Positive Technologies основана на анализе поведения собственных клиентов, а также учитывающая публичные и инсайдерские данные о бюджетах 2022 года, потраченных на те или иные средства защиты информации отечественными компаниями.

Прогнозы на 2023 год

По итогам событий 2022 года индустрия кибербезопасности подошла к необходимости переосознания основных принципов построения защиты и реагирования на угрозы в масштабах бизнеса, отраслей и страны, и в 2023 году кибербезопасность как индустрию ожидает период активной пересборки с большей ориентированностью на практику результативной защиты.

В ближайшие годы рынок ИБ в России окончательно станет рынком отечественных производителей и будет расти в разы, еще больше возрастет востребованность технологий, позволяющих предотвращать хакерские атаки до того, как компаниям будет нанесен непоправимый ущерб. В частности, трендом следующего года можно считать рост интереса к платформам Bug Bounty у компаний различных сфер бизнеса (включая государственные), практическим киберучениям и средствам защиты с максимальным уровнем автоматизации в части выявления хакерских атак и противодействия им.
Также на промежутке 1—2 лет стоит ожидать появления на рынке новых прогрессивных средств защиты в нишах, традиционно занимаемых до сих пор зарубежными игроками. Так, в первую очередь мы увидим обновления линеек решений в классе NGFW, защиты контейнерных сред и облаков.

Главные итоги и тренды законотворчества в сфере ИБ

Артем Сычев, советник генерального директора Positive Technologies

С точки зрения нормативно-законодательного направления безусловно важным событием в 2022 году стал выход 250-го указа Президента «О дополнительных мерах по обеспечению информационной безопасности РФ». Данный документ придал развитию ИБ определенный импульс, который нужно в дальнейшем поддержать. Это та искра, из которой должно разгореться пламя, но для этого нужны правильные «дрова».

Вторым важным моментом стали серьезные дискуссии вокруг оборотных штрафов, связанные с утечками персональных данных. Ответственность действительно должна ужесточаться. Сомнений в этом никаких нет, но вопрос в том, как убедиться, что утечка произошла действительно по вине оператора, а не потому, что злоумышленник воспользовался какой-то лазейкой, о которой никто и подумать не мог? Камнем преткновения становится доказательство вины оператора.

К концу года правительство также утвердило Концепцию формирования и развития культуры информационной безопасности граждан РФ. Причина появления этого документа очень проста: большинство событий по информационной безопасности происходят даже не потому, что где-то что-то не было настроено или пропатчено (не обновлено), а из-за влияния человеческого фактора. Люди часто не понимают сути тех технологий, которые они используют, и поэтому не осознают связанные с этим риски, ведутся на фишинговые атаки, мошеннические звонки или серфинг по сомнительным сайтам. В итоге происходят те самые инциденты. По сути, лечится это активной пропагандой киберкультуры и кибергигиены. Отрадно, что правительство этой темой озаботилось.

Прогнозы на 2023 год

Если попытаться спрогнозировать изменения в законодательной и нормативно-правовой базе в области информационной безопасности в новом году, то можно выделить четыре основных тренда:

Развитие 250-го указа. В его поддержку должны появиться некоторые методологические документы и практика применения мер воздействия к тем, кто начинает пренебрегать ИБ. Этот указ впервые вывел кибербезопасность на уровень руководящего звена и владельцев бизнеса. Российское законодательство и нормативная база, к сожалению, не оперирует таким понятием, как «недопустимые события». Крайне важно, чтобы оно под этим или каким-то иным названием появилось в законодательстве и нашло свое отражение в целой цепочке нормативных актов: от приказов ФСТЭК до методических рекомендаций Минцифры.

Легализация отраслевых центров ГосСОПКА. Здесь важно, чтобы федеральные органы исполнительной власти, которые курируют те или иные отрасли экономики, получили определенные полномочия для продвижения идей ИБ в своих подведомственных отраслях. Это совершенно точно невозможно без внесения изменений в законодательство. 250-й указ запустил процесс аккредитации центров ГосСОПКА, а перед ФСБ России стоит задача по нормативному оформлению этого процесса. Наша компания также активно участвует в реализации этой задачи и сможет привнести в нее практические вещи, связанные с информационной безопасностью. По сути, центры ГосСОПКА — отраслевые или относящиеся к конкретному предприятию — точно так же должны выполнять элементарные требования информационной безопасности и должны быть проверены на устойчивость к атакам. Это тоже тренд нового года.

Продолжение эксперимента. В новом году, вероятно, эксперимент по апробации работоспособности подхода результативной безопасности, который сейчас проводит Минцифры в рамках некоторых государственных информационных систем согласно постановлению правительства №860, должен получить распространение. Этот вопрос тоже потребует определенного нормативного регулирования.

Киберграмотность. Особое внимание в 2023 году следует уделять вопросам обучения и киберкультуры. Лидеры отрасли кибербезопасности должны стать активными участниками этого процесса, чтобы донести до простых пользователей все правила безопасного использования информационных технологий. Им необходимо принять участие в обучении большого количества негосударственных служащих, сформировать инструменты доступной коммуникации для широких слоев общества на тему того, что такое информационная безопасность.

Смена парадигмы ИБ, переход к результативной защите и что еще принесет 2023 год

Алексей Лукацкий, бизнес-консультант
по информационной безопасности, Positive Technologies

Даже в условиях волатильного рынка и изменчивой общественно-политической обстановки в 2023 году можно выделить ряд сформировавшихся трендов, актуальных для отечественных компаний.

Усиление защиты персональных данных

Львиная доля последствий всех атак в течение года (почти в половине атак на организации и более 60%, когда речь идет об атаках на частных лиц)[1] приходится на утечки конфиденциальной информации, в том числе и персональных данных. Это повлекло за собой существенный рост внимания к защите личной информации со стороны государства, которое предложило ряд законодательных инициатив. Некоторые из них будут рассмотрены в весеннюю сессию Госдумы: в первую очередь речь идет об оборотных штрафах за утечки персональных данных и уголовном преследовании за их незаконный оборот. Стоит отметить, что с 1 сентября 2022 года вступили в силу новые требования Федерального закона № 152. Они обязывают компании в течение суток уведомлять ФСБ и Роскомнадзор о произошедших утечках персональных данных.

Рост числа утечек с одной стороны и оборотные штрафы с другой, вероятно, заставят российские предприятия задуматься о пересмотре своей архитектуры защиты данных, а также о выстраивании процесса управления инцидентами для своевременного уведомления о них. Требование об уведомлении в течение 24 часов, независимо от праздников и выходных, — это серьезный вызов даже для опытных в управлении кибербезопасностью компаний.

Нехватка кадров станет драйвером сервисной модели и автоматизации в ИБ

Исторический кадровый голод в области ИБ и актуальный запрос на практическую кибербезопасность будут, с одной стороны, стимулировать развитие рынка MSSP[2], а с другой — формировать запрос на появление технологий с высокой автоматизацией противодействия киберугрозам, когда роль оператора продуктов ИБ будет все больше замещаться технологиями автоматического противодействия атакам.

Новая норма об уведомлении ФСБ и Роскомнадзора об утечках персональных данных в течение суток распространяется на 8 миллионов предприятий — от органов власти и компаний первого эшелона до индивидуальных предпринимателей. Если добавить к этому требование вышедшего в мае 2022 года президентского Указа № 250 о наличии почти в полумиллионе российских организаций заместителя генерального директора, ответственного за кибербезопасность, а также отдельной службы ИБ, то ситуация становится еще более сложной — в России сейчас просто нет такого количества специалистов по ИБ.

[1] Общемировые данные, основанные на собственной экспертизе компании, результатах расследований, а также на данных авторитетных источников.

[2] Managed Security Service Provider – безопасность как сервис, или доступ к передовым технологиям и квалифицированным экспертам в области инфобеза за приемлемые деньги.

Решение этой проблемы развивается по двум направлениям:

1. сервисная модель ИБ, предполагающая оказание услуг кибербезопасности (всех или только некоторых) внешним поставщиком, который обладает квалифицированным персоналом и реализует все необходимые, а также предусмотренные законодательством функции;

2. автоматизация рутинных задач за счет использования специализированного ПО (например, системы класса SOAR[1]) или отдельных модулей и функций в существующем ПО (например, SIEM[2], NDR[3] или WAF[4]), позволяющих решить большинство задач ИБ силами существующих специалистов, а также использование уникальных средств защиты, основанных на применении ML-технологий, способных предотвращать хакерские атаки и требующих для этого буквально одного-двух экспертов ИБ.

Новые старые продукты ИБ

Уход иностранных компаний по ИБ поставил перед многими российскими предприятиями дилемму — продолжать использовать необновляемые средства защиты или найти им замену. В первом случае проблема будет решаться обращением к зарождающемуся в России рынку threat content as a service, в рамках которого для решений ушедших вендоров ИБ создается контент для обнаружения угроз (сигнатуры атак, индикаторы компрометации, правила YARA и SIGMA и т. п.), что позволяет снизить риски превращения используемых решений с неистекшими лицензиями в неработающие продукты.

Во втором случае проблема решается миграцией с решений Cisco, Palo Alto, Fortinet, IBM, Micro Focus, Trend Micro и др. на отечественные аналоги. Учитывая требования 250-го Указа Президента, запрещающего с 1 января 2025 года закупать иностранные средства защиты, этот год пройдет у российских организаций под знаком поиска подходящих альтернатив. Будут заменяться первоочередные решения в области ИБ — межсетевые экраны следующего поколения (NGFW), системы мониторинга событий ИБ (SIEM), системы мониторинга сетевых аномалий и атак (NDR), системы защиты оконечных устройств (XDR), межсетевые экраны для веб-приложений (WAF), сканеры безопасности, средства идентификации и аутентификации, системы предотвращения вторжений.

В 2023 году придут новые аббревиатуры и продуктовые категории, а также большое внимание клиентов и производителей к следующим направлениям:

- защита и мониторинг безопасности растущего сегмента децентрализованного интернета — Web3;
- безопасность API, а также интеграция этой функции с механизмами защиты от ботов, решениями класса RASP[5] (runtime application security protection), средствами защиты от DDoS-атак, а также WAF;
- защита решений по автоматизации разработки без программирования — no-code/low-code;
- визуализация атак (решения класса attack path visualization). Эти решения стали разрабатываться и на российском рынке;
- учитывая число инцидентов с системами идентификации и многофакторной аутентификации, которыми ознаменовался 2022 год, возникнет интерес к решениям класса IDR (identity detection and response), по аналогии с NDR, XDR, CDR[6], EDR[7] и т. п.;

[1] Система оркестрации, автоматизации, реагирования на инциденты информационной безопасности.
[2] Система мониторинга событий ИБ и выявления инцидентов.
[3] Система мониторинга сетевых аномалий и атак.
[4] Система мониторинга событий ИБ и выявления инцидентов.
[5] Защита безопасности приложений во время их выполнения.
[6] Обнаружение и реагирование в облаке.
[7] Решение для защиты конечных точек (рабочих станций, серверов, устройств Интернета вещей).

- обнаружение недостоверной информации и фейков в интернете;
- zero trust (организация сетевого доступа к корпоративным ресурсам с нулевым доверием) и BYOD (IT-политика, которая позволяет и даже поощряет использование собственных устройств для выполнения рабочих задач). Учитывая новый виток перехода на удаленную работу, данные решения будут востребованы и в России.

Год под знаком ChatGPT

Отдельно хотелось бы отметить технологии машинного обучения, а именно генеративного искусственного интеллекта, которые ворвались в 2022 год с проектами DALL-E, Midjourney, ChatGPT и т. п. Специалисты уже задаются вопросом: какую следующую креативную профессию мы собираемся ~~уничтожить~~ автоматизировать? В 2023 году этот вопрос встанет и перед ИБ. Уже сегодня генеративный ИИ может искать уязвимости, писать политики ИБ и правила для систем обнаружения угроз, проводить анализ вредоносного ПО, автоматизировать проведение пентестов и поиск уязвимостей и многое другое. В России проекты OpenAI недоступны, но в интернете можно найти много реплик с них, позволяющих построить облегченные модели машинного обучения с возможным применением в ИБ. В этом году такие проекты станут появляться и у отечественных компаний, специализирующихся на ИБ.

Результативная кибербезопасность

Нехватка кадров, рост числа атак, недостаток решений ИБ, уход иностранных игроков, увеличение числа уязвимостей… Все это заставляет российские компании (да и не только российские) менять парадигму обеспечения кибербезопасности в пользу обеспечения цифровой устойчивости предприятия, которая обеспечивается не абсолютно везде и на одинаковом уровне, а там, где находятся самые ценные активы компании, негативное кибервоздействие на которые может привести к реализации недопустимых для бизнеса событий с катастрофическими последствиями. Эта концепция позволяет сфокусироваться на самом важном для бизнеса, что особенно необходимо в текущих условиях, в которых российские компании будут существовать весь 2023 год.

Кто и как атакует российские организации

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

Новые кибергруппировки, успешные взломы и утечки данных

В 2022 году сотрудники экспертного центра безопасности Positive Technologies провели более 50 расследований. Пик по количеству инцидентов пришелся на апрель 2022 года. Результативность кибератак осталась на прежнем уровне: количество атак возросло, но, к сожалению, увеличилось и число успешных взломов. Причин этому несколько: рост числа уязвимостей и их неустранение, нехватка кадров более чем у 90% компаний, уход иностранных вендоров ИБ. В некоторых атаках злоумышленникам удалось реализовать недопустимые для компаний событий, например остановить бизнес-процессы.

Уровень сложности зафиксированных нами атак ранжируется от школьников до проправительственных APT-группировок. Больше половины инцидентов было совершено квалифицированными злоумышленниками. 20% случаев составили атаки типа supply chain и trusted relationship, которые сложно расследовать специалистам по ИБ. Мы наблюдаем интересную тенденцию: злоумышленники не изобретают новые способы атак, но тем не менее число инцидентов с применением уже известных методов продолжает расти.

За большинством атак в 2022 году стояли политически мотивированные хактивисты — встречались как хакеры-одиночки, так и спонтанно организованные группы, которые преимущественно состояли из разрозненных энтузиастов. Для атаки им достаточно иметь ноутбук с подключением к интернету (таким образом, например, проводятся DDoS-атаки). Организаторы подобных сообществ координируют участников и направляют их активность на заранее выбранные цели. Чаще всего в прошлом году целями подобных атак становились государственные учреждения и СМИ. Таким способом преступники пытались вызвать общественный резонанс и панические настроения среди населения. В ближайшее время хактивизм вряд ли пойдет на спад. Более того, мы ожидаем усложнение таких атак, поскольку многие российские компании осознали важность кибербезопасности и начали укреплять защиту своего периметра.

Продолжают быть активными APT-группы, в частности APT31, Cloud Atlas и Space Pirates. По итогам проведенных нами расследований, отраслевые интересы группировок, атаковавших российские организации в течение 2022 года, распределились между государственными предприятиями (30% случаев), IT-компаниями (16%), финансовым, энергетическим и промышленным сектором (по 10% случаев на каждый). Кроме того, в 2022-м претерпел изменения ландшафт кибергруппировок, нацеленных на отечественный сегмент. Ранее новые высококвалифицированные преступные объединения возникали достаточно редко, поэтому мы могли быстро атрибутировать ту или иную атаку к уже знакомым APT-группировкам по инструментам, тактикам и техникам, применяемым при нападении. В прошлом году было обнаружено большое количество ранее неизвестных кибергрупп. Любопытно, что некоторые из них деанонимизировали себя в социальных сетях, раскрывая свою причастность к совершенным атакам. Чаще всего целями атак становилось хищение и «слив» данных в интернет, чтобы нанести репутационный ущерб жертвам. Большая часть новопоявившихся групп никакой выгоды не преследовала, взломы они совершали только ради хайпа. К концу года ценность данных серьезно возросла, из-за чего «сливы» стали происходить значительно реже, чем в первом полугодии.

Фишинг, уязвимости и кросс-платформенные хакерские инструменты

Верхние строчки в топе наиболее популярных и эффективных способов проникновения в компании, как и в предыдущие годы, занимает взлом периметра и фишинг. В числе уязвимостей, которые наиболее активно использовались для проникновения в инфраструктуру, были бреши в серверах Microsoft Exchange, Log4Shell, ProxyNotShell и ProxyShell. Отдельного внимания заслуживает достаточно серьезная уязвимость CVE-2022-30190, также известная как Follina, в Microsoft Windows Support Diagnostic Tool (MSDT). Она может быть проэксплуатирована при помощи вредоносного офисного документа и позволяет злоумышленникам выполнить произвольный код.

Касательно новых техник киберпреступников, стоит отметить атаки через опенсорс. Их число растет, однако в нашей практике мы пока не видели ни одной успешной реализации.

По нашим данным, в атаках с применением вредоносного ПО самыми эффективными были инфостилеры, шифровальщики и вайперы. Они позволяют злоумышленникам быстро получить доступ в инфраструктуру жертвы, не тратя время на поиск уязвимостей нулевого дня, и похитить данные. Помимо этого, все больше хакерских инструментов и вредоносного ПО стали писать на кросс-платформенных языках, например Go и Rust. Это упрощает компиляцию под различные операционные системы.

Прогнозы на 2023

Под угрозой все

Атаки киберпреступников в ушедшем году изменили сложившиеся стереотипы о том, что их интересует только финансовая нажива. Под ударом оказались даже те компании, которые исторически считали себя неинтересными для злоумышленников. В 2023 году стоит ожидать развития подобной активности в отношении российских организаций, в том числе от известных кибергруппировок. Помимо этого, мы не исключаем появления новых APT-групп, уязвимостей нулевого дня, а также активизацию «спящих» инцидентов. Это требует от всех организаций переосмыслить отношение к кибербезопасности, обозначить самые неприемлемые для их бизнеса события и исключить возможность их реализации в результате кибератаки.

Интерес злоумышленников к отечественным ОС возрастет

По нашим прогнозам, одним из ярких трендов 2023 года станет активный поиск уязвимостей нулевого дня в отечественных операционных системах (Astra Linux, ALT Linux, РЕД ОС).

Атаки через зависимости в продуктах с открытым исходным кодом

Усилится тренд атак, связанный с доставкой вредоносного кода в открытом ПО через сторонние зависимости. В прошлом году выросло число зловредов, распространяемых через опенсорс. Основные источники такого ВПО — репозитории с пакетами для разработки, в частности PyPi и NPM. В них, как правило, содержатся стилеры[1] учетных записей, данных банковских карт и криптовалюты. Для обнаружения подозрительных и вредоносных Python-пакетов мы рекомендуем использовать специальные сервисы. В 2023 году также останется актуальным использование легитимных сервисов (облаков, мессенджеров) в качестве контрольного сервера. Этот способ сейчас популярен не только у APT-группировок, но и менее квалифицированных злоумышленников.

[1] ВПО для кражи паролей пользователей.

Многофакторная аутентификация уже не панацея

Почти каждая вторая атака в 2022 году приводила к потере конфиденциальных данных. Массовые утечки данных, в том числе учетных данных, приведут к увеличению числа атак и на второй фактор аутентификации. Уже сейчас злоумышленники находят способы обходить многофакторную аутентификацию путем фишинга, обмана пользователей с помощью социальной инженерии, взлома поставщиков решений для аутентификации (стоит вспомнить взлом компании Okta, который задел ее клиентов). Организациям следует убедиться в надежности используемых решений для аутентификации пользователей.

Шифровальщики и вайперы не отступают

Атаки шифровальщиков наносили серьезный ущерб как отдельным организациям, так и государственным структурам и целым отраслям. Но количество атак шифровальщиков снизилось на 15% по сравнению с 2021 годом. Жертвами чаще всего становились госучреждения, промышленные предприятия, медицинские организации, научные и образовательные учреждения.

Оценивая развитие подобных атак в 2022 году, мы прогнозировали, что некоторые преступники переключатся на организации среднего уровня, пожертвовав крупными суммами выкупа, но с расчетом на большее число жертв и более «спокойную» деятельность, пока у спецслужб в приоритете более серьезные группировки. Также мы предполагали, что организации будут чаще отказываться платить выкуп. Действительно, в 2022 году было значительно меньше резонансных атак, существенно уменьшилась средняя сумма выкупа и выросло количество отказов от выплат. По данным отчета Coveware, средняя сумма выкупа, которая была выплачена вымогателям в первом полугодии 2022 года, составила 228 тысяч долларов, при этом медианная выплата составила около 36 тысяч долларов, что меньше показателя конца 2021 года на 51%.

Злоумышленники находили новые способы давления на жертв, чтобы уменьшить число отказов: дефейс корпоративных сайтов, создание платформ со списками похищенной информации в открытом доступе, чтобы сотрудники и клиенты компаний могли проверить, есть ли их данные среди украденной информации.

В начале 2022 года некоторые группировки шифровальщиков переключились с требования выкупа на необратимое повреждение инфраструктуры жертвы. С начала года увеличилось количество атак с использованием ПО для удаления данных. В целом для организаций их доля составила 2%, но больше всего от применения вайперов пострадали промышленные предприятия, где вайперы были замечены в 7% атак с использованием ВПО. Среди таких «очистителей» данных можно отметить WhisperGate, HermeticWiper, IsaacWiper, DoubleZero, CaddyWiper. Вредоносное ПО может имитировать атаку программы-вымогателя, однако жертвы не получат ключи для дешифрования, а данные будут необратимо повреждены. Распространение вайперов ожидается и в 2023 году.

В то же время продолжаются атаки, нацеленные на кражу данных без шифрования инфраструктуры с последующим требованием выкупа за неразглашение украденной информации. Пока мы не увидели усиления этого тренда, однако не исключаем этого в следующем году.

Теневой рынок доступов: киберпреступники активно осваивают Telegram

Теневой рынок преступных киберуслуг стал наращивать присутствие в мессенджерах, которые удобны для использования широкой аудиторией и обеспечивают приемлемый уровень анонимности меньшими усилиями.

Теневые площадки все чаще создают каналы и группы в Telegram, и в середине 2022 года мы зафиксировали рекордное количество сообщений подобного рода в мессенджере. В основном здесь идет торговля данными, вредоносным ПО, продвигаются разного рода услуги киберпреступников: взлом ресурсов (в том числе сайтов, почтовых аккаунтов и аккаунтов в социальных сетях), обналичивание средств, распространение ВПО, спам-рассылки, услуги DDoS. Активность в мессенджере хорошо отражает основные тренды в киберпреступной среде. Например, значительный рост числа сообщений на тему DDoS пришелся на I квартал 2022 года, когда мы наблюдали рост числа атак на веб-ресурсы различных организаций. В первом полугодии 2022 года на фоне многочисленных атак и утечек данных преобладающей стала тема документов, персональных данных и услуг, связанных с ними.

Такой вектор развития криминальных площадок еще больше снижает порог входа для новых участников, а значит, скажется на развитии взаимосвязей между преступными группировками, облегчит торговлю украденными данными и вредоносным ПО, поиск исполнителей атак. Тем не менее наиболее серьезные операции, в том числе распространение известных шифровальщиков, торговля доступами к корпоративным сетям, практически не выносятся в публичные каналы, а совершаются в рамках закрытых партнерских программ и специализированных форумов.

Уязвимости ради безопасности

Вадим Соловьев, руководитель группы анализа угроз ИБ, Positive Technologies

Результативная стратегия управления уязвимостями

В 2022 году установлен отрицательный рекорд — по данным базы CVE[1], верифицировано порядка 25 тысяч новых уязвимостей, обнаруженных исследователями безопасности. Уязвимостям были присвоены соответствующие идентификаторы и уровни опасности согласно международному стандарту CVE. Рост числа стартапов и выпускаемых ими программ, а также несоблюдение принципов безопасной разработки может привести к тому, что в 2023 году будет установлен новый антирекорд.

Почти 70 уязвимостей в день — это много. В России этот показатель усугубляется еще и тем, что иностранные ИТ-компании ушли из страны и прекратили поставлять новые версии и обновления для своего ПО, оставляя отечественные предприятия беззащитными, что в свою очередь поднимает вопрос о выстраивании результативной стратегии управления уязвимостями — как в проприетарном ПО, так и в используемых компонентах с открытым исходным кодом, причем не только в веб-приложениях, но и в программах собственной разработки.

К числу популярных уязвимостей в 2022 году, о которых много говорили в среде ИБ, относились:

- Log4j (CVE-2021-44228),
- ProxyNotShell (CVE-2022-41040),
- Spring4Shell (CVE-2022-22965),
- Atlassian Confluence (CVE-2022-26134, CVE-2022-26138),
- Zimbra RCE (CVE-2022-27925, CVE-2022-41352),
- Follina web framework Ruby on Rails (CVE-2022-30190),
- F5 BIG-IP (CVE-2022-1388).

Наиболее критические уязвимости, которые чаще всего обсуждали в дарквебе:

[1] Common Vulnerabilities and Exposures — база данных общеизвестных уязвимостей ИБ, поддерживаемая корпорацией MITRE.

Трендовые уязвимости 2022 года

Тип уязвимости	Вендор	Идентификатор уязвимости	Оценка базовой метрики вектора CVSS
Обход аудентификации	Fortinet	CVE-2022-40684	9,8
RCE	VMware	CVE-2022-22965	9,8
LPE	Linux	CVE-2022-0847	7,8
RCE	Microsoft Corporation	CVE-2022-30190	7,8
RCE	VMware	CVE-2022-22954	9,8

Прогнозы на 2023

Мы ожидаем, что Log4Shell, Spring4Shell и подобные им уязвимости еще долго будут с нами, так как системы, использующие уязвимое ПО, широко распространены. Кроме того, в 2023 году мы вновь увидим атаки на Microsoft Exchange как через новые уязвимости, так и через старые, которые пользователи все еще не устранили с помощью обновлений безопасности.

Наибольшую ценность для злоумышленников будут представлять уязвимости в браузерах, поскольку через них можно проводить массовые атаки на посетителей конкретных ресурсов, и уязвимости в популярных фреймворках, которые активно используются в том числе в инфраструктуре крупных компании. Отдельно стоит отметить окончание поддержки Windows 8.1 с 10 января 2023 года. Для этой операционной системы перестанут приходить обновления безопасности. Поэтому в случае выявления уязвимостей в базовых механизмах ОС семейства Windows, пользователи старых версий ОС (в том числе Windows 8.1) окажутся незащищены.

Неизвестные разработчикам уязвимости

Проблемы, связанные с уходом зарубежных производителей ПО, отсутствием обновлений безопасности, нарушением привычных цепочек поставок ПО, продолжат оказывать влияние на информационную безопасность в компаниях в 2023 году. Разрыв связей между разработчиками и исследователями безопасности из разных стран приведет к тому, что в ПО будет значительно больше уязвимостей, о которых не знают разработчики, но которые могут быть выявлены злоумышленниками. Негативный эффект на уровень защищенности организаций будет оказывать необходимость выстраивать новые цепочки поставок ПО и интегрировать в инфраструктуру новые решения, безопасность которых может быть под вопросом.

Самые громкие атаки и самые атакуемые отрасли

Топ-10 самых громких атак 2022 года

1 **Атака вымогателей на госучреждения Коста-Рики**

Беспрецедентный случай атаки на госучреждения произошел в апреле: группировка вымогателей Conti напала на госучреждения Коста-Рики и потребовала выкуп в 20 млн долларов. Из-за недоступности большей части IT-инфраструктуры в стране было объявлено чрезвычайное положение, а несколько позже к атакованному государственному сектору присоединилось здравоохранение Коста-Рики, управление и учреждения которого атаковала группировка Hive.

2 **Атаки Lapsus$ на Okta, Nvidia, Microsoft, Samsung и другие компании**

Группировка Lapsus$ взломала ряд крупных IT-компаний, в числе которых оказались Okta, Nvidia, Microsoft, Samsung. В начале года была атакована Okta, которая разрабатывает решения для управления учетными записями и доступами, в том числе обеспечивает поддержку многофакторной аутентификации. Атака задела около 2,5% клиентов компании и поставила под сомнение надежность решений, которые используются для аутентификации. В феврале Lapsus$ атаковали разработчика графических процессоров Nvidia. В результате атаки был украден 1 ТБ данных, среди которых были исходный код драйверов видеокарт и сертификаты для подписи ПО. Украденные сертификаты Nvidia использовались злоумышленниками для распространения вредоносных программ, в том числе бэкдоров и троянов удаленного доступа. В марте преступники взломали компании Microsoft и Samsung и украли исходный код некоторых продуктов.

3 **Атака на Swissport International**

Швейцарская компания Swissport International, провайдер наземного обслуживания и грузовых авиаперевозок, которая работает в 310 аэропортах в 50 странах мира, подверглась атаке программы-вымогателя. Атака привела к задержкам множества рейсов. Кроме того, преступники украли 1,6 ТБ данных.

4 **Атака на Vodafone Portugal**

Атака на телекоммуникационного оператора Vodafone в Португалии вызвала сбои в обслуживании по всей стране, в том числе в работе сетей 4G и 5G, а также при передаче SMS-сообщений и предоставлении телевизионных услуг. Vodafone Portugal обслуживает более 4 млн абонентов сотовой связи в стране и еще 3,4 млн интернет-пользователей, поэтому масштабы последствий атаки почувствовали многие граждане Португалии. Компании потребовалось много времени на восстановление своих систем: например, сайты организации снова стали функционировать спустя почти месяц.

5 **Утечка данных граждан Индонезии**

На одном из теневых форумов на продажу был выставлен архив, содержащий набор данных о 105 млн граждан Индонезии — это почти 40% населения страны. Предполагается, что информация была украдена из «Всеобщей избирательной комиссии». Архив содержит полные имена, даты рождения и другую личную информацию, а назначенная злоумышленником цена составляет 5000 долларов. Ранее преступник также выложил архив, содержащий регистрационные данные около 1,3 млрд SIM-карт, — номера телефонов, удостоверения личности — стоимостью 50 000 долларов.

6 **Кража денег у блокчейн-системы Ronin**

В марте произошла атака на сайдчейн Ronin компании Axie Infinity, которую на данный момент можно считать крупнейшим взломом среди децентрализованных криптовалютных систем. Злоумышленникам удалось вывести почти 620 млн долларов в токенах Ethereum и USDC.

7 **Атаки на немецкие нефтяные компании Oiltanking и Mabanaft, нефтяные терминалы в Бельгии и Нидерландах**

В конце января жертвами кибератак стали две дочерние компании группы Marquard & Bahls — немецкий дистрибьютор бензина Oiltanking и поставщик нефти Mabanaft. Многие автоматизированные технологические процессы, связанные с загрузкой и разгрузкой резервуаров, полностью зависят от компьютерных систем, которые какое-то время были отключены. В результате компании временно не могли выполнять договорные обязательства. Несколькими днями позже были атакованы крупные нефтяные терминалы SEA-Invest в Бельгии и Evos в Нидерландах. Эти события повлияли на работу портов во всей Европе и Африке и привели к задержкам поставок топлива.

8 **Остановка поездов в Дании**

В октябре в результате кибератаки на Supeo, поставщика IT-услуг для крупнейшей датской железнодорожной компании, на несколько часов остановилось движение поездов.

9 **Остановка заводов Toyota**

В марте Toyota на день приостановила работу 14 заводов в Японии из-за кибератаки на Kojima Industries, поставщика компонентов для производства автомобилей.

10 **Множественные утечки данных российских пользователей**

В течение года произошло множество утечек персональных данных российских пользователей, в том числе из популярных сервисов и крупных компаний. Среди наиболее известных — «Яндекс.Еда», Delivery Club, «Гемотест» , «ВкусВилл», Whoosh, «СДЭК», DNS, Level.Travel.

Государственные организации — цель №1

Екатерина Килюшева, руководитель исследовательской группы отдела аналитики информационной безопасности, Positive Technologies

В I квартале 2022 года количество атак, направленных на госучреждения, увеличилось практически в два раза по сравнению с последним кварталом 2021 года, а затем продолжало расти в течение всего года. Государственные учреждения столкнулись с наибольшим количеством кибератак среди организаций: их доля от общего числа атак составила 17%, это на 2 п. п. больше, чем в 2021 году. Всего за 2022 год мы зафиксировали 403 атаки, что на 25% больше, чем за 2021 год[1].

[1] Общемировые данные, основанные на собственной экспертизе компании, результатах расследований, а также на данных авторитетных источников.

Государственный сектор был целью множества преступных группировок, как вымогателей, так и APT-группировок, в числе которых Cloud Atlas, Tonto, Gamaredon, MuddyWater, Mustang Panda. Злоумышленники использовали вредоносное ПО почти в каждой второй атаке на госучреждения. Наиболее популярными типами вредоносов оказались шифровальщики (56% среди атак с применением ВПО) и вредоносные программы для удаленного управления (29%).

Основным вектором атак осталась социальная инженерия, с помощью которой злоумышленники заражали компьютеры сотрудников вредоносным ПО, похищали учетные данные. В середине года мы отмечали всплеск атак на веб-ресурсы государственных учреждений, суммарно на них был направлен 41% атак. По сравнению с 2012 годом это значение выросло на 16 п. п. В 5% атак госучреждения становились жертвой компрометации цепочки поставок ПО.

Действия злоумышленников в каждой третьей атаке приводили к утечке конфиденциальной информации, в том числе персональных данных граждан. С нарушением деятельности в том или ином виде столкнулись учреждения более чем в половине случаев. В 41% случаев атаки приводили к нарушению интересов государства, например, из-за недоступности важных IT-систем или утечек информации о гражданах. Беспрецедентный случай произошел в апреле, когда группировка вымогателей Conti потребовала выкуп 20 млн долларов у правительства Коста-Рики — из-за недоступности большей части IT-инфраструктуры в стране было объявлено чрезвычайное положение. Атака вымогателей на администрацию итальянского Палермо привела к отключению всех IT-систем, что повлекло за собой целый спектр проблем из-за недоступности веб-сервисов: перебои в работе госучреждений, полицейских участков, городского видеонаблюдения, невозможность оплатить проезд в транспорте.

Прогнозы на 2023: расцвет хактивизма

Мы ожидаем дальнейшего увеличения числа атак на государственные структуры. За ними будут стоять как организованные высококвалифицированные кибергруппировки, нацеленные на кражу ценных данных, получение финансовой выгоды, нарушение работы государственных систем, так и хактивисты. Хактивизм тоже может привести к негативным последствиям, от дефейса сайтов до разрушения инфраструктуры. Цифровизация большинства услуг для населения без должной защиты от кибератак ставит под угрозу персональные данные граждан, открывает возможности для модификации данных в государственных системах злоумышленниками, может привести к перебоям в предоставлении услуг, как это уже случалось в 2022 году.

Медицина лидирует по утечкам данных

Медучреждения уже пятый год подряд остаются в тройке самых атакуемых отраслей: в 2022 году доля атак на них составила 9% среди всех организаций, а количество атак держится примерно на уровне 2021 года. Медучреждения чаще всего становились источником утечек данных среди организаций[1].

В более чем 80% случаев атаки приводили к утечкам данных о клиентах: в основном персональных данных и медицинской информации. В системах медучреждений содержатся большие объемы данных, и обычно преступники могут получить следующие сведения: ФИО, дату рождения, физический адрес, телефонный номер, реквизиты счетов и номера карт, информацию о страховке, номер водительского удостоверения, адрес электронной почты, историю болезни, данные о состоянии здоровья и другую медицинскую информацию. В России резонансным стал инцидент с утечкой данных клиентов лаборатории «Гемотест», а именно персональных данных и результатов анализов.

Каждая третья атака становилась причиной перебоев в функционировании рабочих процессов, причем иногда их последствия затрагивали не только отдельные учреждения, но и целое государство. Например, из-за кибератаки на IT-инфраструктуру здравоохранения Гренландии было ограничено оказание всех медицинских услуг на территории острова в течение двух недель.

[1] Общемировые данные, основанные на собственной экспертизе компании, результатах расследований, а также на данных авторитетных источников.

В половине атак использовалось вредоносное ПО, преимущественно шифровальщики. Среди самых распространенных — Conti, Avos Locker, BlackBasta, Hive. Чаще всего злоумышленники доставляли ВПО через электронную почту с использованием приемов социальной инженерии и путем эксплуатации уязвимостей на сетевом периметре. Достаточно высок процент атак (26%), в которых доступ к инфраструктуре был получен путем компрометации корпоративных учетных данных, что говорит как о слабости парольной политики и недостаточном внедрении двухфакторной аутентификации, так и об эффективности фишинговых атак на сотрудников. В четверти атак злоумышленники использовали недостатки защиты ресурсов на периметре организаций.

Прогнозы на 2023

Атаки злоумышленников, нацеленные на кражу конфиденциальных данных, продолжатся в 2023 году. Следует убедиться, что приняты все необходимые меры по обеспечению безопасности конфиденциальных данных, поскольку сейчас медицинские организации показывают не самый высокий уровень защищенности. Вероятны и фишинговые атаки непосредственно на клиентов клиник с целью получения учетных данных от личных кабинетов, в которых хранятся персональные данные и истории болезни, поэтому необходимо вводить строгие методы аутентификации, внедрять обязательную двухфакторную аутентификацию для клиентских сервисов.

С другой стороны, на медучреждения будет оказывать давление деятельность шифровальщиков, а значит, им необходимо обеспечить бесперебойную работу внутренних сервисов даже в условиях взлома инфраструктуры, а также возможность в кратчайшие сроки восстанавливать ее работоспособность. Новые векторы атак открываются с распространением телемедицины: можно ожидать атаки, направленные на взлом сервисов и приложений, используемых для оказания дистанционных услуг.

Атаки, направленные на взлом медицинских устройств личного пользования, вряд ли станут массовыми в ближайшее время. Но эти устройства могут стать целями для высокотаргетированных атак.

Тем не менее вендорам следует еще на этапе разработки позаботиться о защищенности медицинских устройств, чтобы избежать массового отзыва в случае обнаружения проблем с безопасностью и всплеска атак.

Промышленный сектор: нацеленность на остановку технологических процессов

Дмитрий Даренский, руководитель практики промышленной кибербезопасности, Positive Technologies

В 2022 году почти каждая десятая атака на организации приходилась на промышленные предприятия. Всего за год зафиксировано 223 атаки на промышленные компании, что на 7% больше по сравнению с 2021 годом[1]. Основной удар по промышленности пришелся на II квартал, когда общее количество атак на организации промышленного сектора увеличилось на 53% вследствие возросшей активности шифровальщиков.

[1] Общемировые данные, основанные на собственной экспертизе компании, результатах расследований, а также на данных авторитетных источников.

Почти в половине атак использовалась социальная инженерия, в 41% атак злоумышленники эксплуатировали уязвимости в ПО. В большинстве атак (71%) применялось вредоносное ПО, которое распространялось преимущественно через компрометацию ресурсов на периметре организаций (49%) и электронную почту (43%). Уже третий год подряд мы отмечаем снижение доли использования социальной инженерии и увеличение доли эксплуатации недостатков защиты на ресурсах периметра. Чаще всего атаки на компании проводились для кражи конфиденциальной информации: в 54% случаев последствием атаки становилась утечка информации, причем сведения, относящиеся к коммерческой тайне, составили более трети от украденных данных. Действия злоумышленников значительно влияли и на основную деятельность компаний, что наносило серьезный ущерб. Перебои в работе из-за вмешательства в технологические и бизнес-процессы случались в 47% атак. В основном это было связано с использованием шифровальщиков и ПО для удаления данных. В течение года доля шифровальщиков среди вредоносного ПО увеличивалась: если в первом квартале она составляла 53%, то в третьем квартале уже 80%. Доля ПО для удаления данных достигла 7%.

Не обошлось без масштабных атак в самых разных отраслях: нефтегазовой отрасли, энергетике, агропромышленности. К примеру, в начале апреля 2022 года атака группировки Conti на Nordex, одного из крупнейших производителей ветряных турбин, привела к шифрованию информационной инфраструктуры компании и масштабному отключению удаленного доступа к управляемым турбинам. Во II квартале произошла крупная атака на три иранских сталелитейных завода, в результате которой были нарушены технологические процессы производства, а на одном из заводов злоумышленникам удалось обрушить ковш с жидким чугуном, что вызвало пожар в цехе. Стоит вспомнить и атаки на российскую агропромышленность: один из крупнейших производителей и дистрибьюторов мясной продукции «Мираторг» подвергся атаке шифровальщика BitLocker, в Ростовской области в результате атаки был временно остановлен завод «Тавр», а в агрохолдинге «Селятино» злоумышленники попытались испортить 40 тысяч тонн продукции, получив несанкционированный доступ к системам, отвечающим за температурный режим хранения замороженной продукции.

При этом некоторые атаки могли повлечь межотраслевые последствия, то есть повлиять на деятельность компаний из других секторов экономики. Например, в начале 2022 года жертвами вымогателей стали две дочерние компании группы Marquard & Bahls: немецкий дистрибьютор бензина Oiltanking и поставщик нефти Mabanaft. Последствия этих атак значительны не только для организаций, но и для обычных граждан: компании снабжают топливом множество заправочных станций страны.

Как изменится ландшафт угроз для промышленных предприятий в 2023 году

Мы полагаем, что целями преступников, стоящих за кибератаками на промышленные предприятия, будут чаще не финансовая выгода или получение крупных сумм выкупа, а перебои деятельности предприятий, остановка важнейших технологических процессов и аварии. В связи с этим мы прогнозируем появление новых вредоносных программ, ориентированных на промышленные системы, а также более широкое применение вайперов, приводящих к уничтожению данных на устройствах. Также мы ожидаем появления новых кампаний кибершпионажа в отношении промышленных предприятий и ТЭК.

Тренды промышленной кибербезопасности в 2023 году

Кибербезопасность как инструмент обеспечения устойчивости производства

Руководители производственных подразделений рассматривают технологии кибербезопасности как один из инструментов, позволяющих обеспечить устойчивую деятельность и требуемый уровень надежности производственных активов, бесперебойность технологических и производственных процессов и, как следствие, плановый объем и качество продукции или сервисов. При этом требования, предъявляемые производственниками к решениям и технологиям ИБ, в первую очередь фокусируются на возможностях обеспечения непрерывности производства и функциональной надежности инфраструктуры и только во вторую очередь — на функциональной и экспертной «начинке» средств защиты. Другими словами, если решение гарантированно обеспечивает стабильную работу предприятия и выполнение производственного плана в текущем ландшафте угроз и в условиях постоянных кибератак, то оно должно включать весь необходимый и достаточный набор функциональных возможностей и экспертизы.

Кибербезопасность как инфраструктурный элемент

На текущий момент подавляющее большинство проектов по модернизации и строительству производственных площадок уже по умолчанию включают решения по обеспечению кибербезопасности. Причем они закладываются в проектах не как дополнительные или наложенные подсистемы, а как инфраструктурный элемент, наравне с сетевым оборудованием, операционными системами, системами хранения данных. Мы ожидаем, что в 2023 году обоснования использования этих решений будут больше ориентироваться не на формальное соответствие требованиям, а на практический смысл и результаты применения технологий ИБ.

Защищенные АСУ ТП от поставщиков

Отечественные разработчики и поставщики программно-технических комплексов промышленной автоматизации постепенно начинают предлагать базовые решения по кибербезопасности, которые уже протестированы и встроены в их экосистемы. Причем эти решения в основном отвечают требованиям как предприятий, так и законодательства в области обеспечения безопасности критической информационной инфраструктуры.

«Неинвазивность» уходит в прошлое

В целом промышленность перестала опасаться средств защиты, которые активно взаимодействуют с компонентами систем промышленной автоматизации и управления производством. Все вопросы к поставщикам и производителям продуктов кибербезопасности, касающиеся данных аспектов, сейчас носят скорее практический характер. Безусловно, предприятиям по-прежнему важно, чтобы кибербезопасность не препятствовала производственной деятельности и не оказывала деструктивного воздействия. При этом на предприятиях конструктивно подходят к задачам реализации функций проактивной защиты и реагирования на инциденты ИБ. Там, где это целесообразно и практически необходимо, применение таких решений рассматривается в рабочем порядке.

Отраслевое регулирование и центры компетенций: начало

В России на сегодняшний день создано 32 индустриальных центра компетенций (ИЦК) и 12 центров компетенций по развитию общесистемного прикладного программного обеспечения. Кроме того, 9 декабря 2022 года Минцифры объявило о создании Центра компетенций по информационной безопасности.

Важно отметить, что последние несколько лет крупнейшие компании из ключевых отраслей промышленности страны начали движение в сторону формализации требований к обеспечению и управлению кибербезопасностью. Основной задачей была адаптация требований законодательства и регуляторов в лице ФСТЭК и ФСБ к отраслевой специфике предприятий и ее учет в формировании методологической основы и нормативно-технической базы в области ИБ.
Предприятия уже получают практические результаты своей работы, и мы надеемся, что они будут использованы для формирования общеотраслевых технических норм обеспечения безопасности и формирования компетенций и правил регулирования кибербезопасности в каждой отрасли промышленности.

Финансовый сектор: наилучшая подготовленность к атакам, но в целом уровень защиты недостаточный

Максим Костиков, руководитель отдела анализа защищенности приложений, Positive Technologies

По итогам 2022 года общее число атак на финансовые организации снизилось на 7% по сравнению с аналогичным периодом 2021 года. Доля атак на финансовую отрасль в последние годы в целом сокращалась и сейчас составляет около 4% от числа всех атак на организации[1].

Чаще всего в атаках используется социальная инженерия (47%). По сравнению с другими отраслями, эксплуатация уязвимостей встречается реже. Скорее всего, это связано с тем, что в целом сетевой периметр финансовых организаций защищен лучше. Поэтому методы социальной инженерии и компрометация учетных данных оказываются более эффективны.

В каждой второй атаке используется вредоносное ПО (в одной атаке могут применяться разные типы ВПО): в основном это загрузчики (59% атак с использованием ВПО), шпионское ПО (18%), шифровальщики (18%) и банковские трояны (12%). В большинстве случаев вредоносное ПО распространяется через электронную почту.

Если рассматривать последствия атак, то финансовые организации чаще всего сталкивались с кражей конфиденциальных данных (53% атак) и остановкой бизнес-процессов (41%). Непосредственные финансовые потери в результате атаки происходили в 6% случаев. В 6% случаев злоумышленники использовали ресурсы финансовой организации для проведения дальнейших атак на клиентов и другие компании.

[1] Общемировые данные, основанные на собственной экспертизе компании, результатах расследований, а также на данных авторитетных источников.

Хотя финансовый сектор лучше всего подготовлен к атакам по сравнению с остальными компаниями, в целом уровень защищенности финансовых организаций от внутреннего и внешнего злоумышленника остается недостаточно высоким. Среди исследованных экспертами Positive Technologies с 2021 по 2022 год финансовых организаций[1] в рамках внешнего пентеста в 86% случаев удалось получить доступ в локальную сеть. Причем в половине из этих организаций проникнуть во внутреннюю сеть компании мог даже злоумышленник, не обладающий высокой степенью подготовки. При проведении внутреннего пентеста во всех случаях экспертам удалось получить полный контроль над инфраструктурой, а также продемонстрировать возможность получения доступа к критически важным системам: например, в одном из банков была выявлена уязвимость, позволяющая скомпрометировать более 1000 банкоматов. Как правило, при проведении верификаций за ограниченный рамками работ период времени удается реализовать более 70% из обозначенных событий.

Прогнозы на 2023: клоны онлайн-банков и атаки через интегрируемые системы

На текущий момент мы не видим предпосылок для появления высококвалифицированных группировок, которые могут осуществлять крупные кражи со счетов банков. В 2022 году злоумышленники продолжали атаковать клиентов онлайн-банков, используя вредоносные программы: банковские трояны, стилеры, программы для удаленного управления. Наиболее опасные трояны позволяют полностью захватить контроль над устройством, перехватывать коды двухфакторной аутентификации и проводить транзакции с того же устройства, которое жертва использует на постоянной основе. Для распространения ВПО и перехвата учетных данных злоумышленники создают клоны онлайн-банков в магазинах приложений, регистрируют поддельные страницы в социальных сетях. В 2023 году стоит ожидать развития подобных атак.

В целом прослеживается тенденция внедрения безопасной разработки онлайн-банкинга на всех этапах производства ПО, что влечет за собой уменьшение стандартных атак на веб-приложения типа OWASP Top 10, но остаются логические уязвимости, которые злоумышленники могут использовать. Эти нетривиальные атаки возможны при глубоком изучении системы и могут привести к хищению денежных средств клиентов, утечке персональных данных и отказе в обслуживании.

Кроме того, банки продолжают расширять экосистему предоставляемых услуг, а значит, у злоумышленников появляется больше возможностей атаковать кредитно-финансовые организации через интегрируемые системы. Это влечет за собой необходимость модернизировать защиту своей экосистемы. Однако уход зарубежных вендоров, в том числе разработчиков средств ИБ, вынуждает IT-службы банков в спешке, зачастую меняя процессы на ходу, внедрять новые решения. В процессе замены обязательно будут ошибки, которые могут сказаться на защищенности компаний.

[1] В выборку вошли проекты по внешнему и внутреннему тестированию, выполненные для организаций кредитно-финансового сектора, в которых заказчики работ не вводили существенных ограничений на перечень тестируемых сетей и систем.

IT-компании: осторожность в использовании открытого ПО и контроль цепочек поставок

Федор Чунижеков, аналитик исследовательской группы отдела аналитики информационной безопасности, Positive Technologies

Число атак на IT-компании в 2022-м несколько уменьшилось по сравнению с 2021 годом, однако на них все еще приходится 6% атак на организации. В течение года мы наблюдали крупные атаки, направленные на IT-компании[1]. Например, в феврале Lapsus$ атаковали американского разработчика графических процессоров Nvidia, а в начале марта под ударом оказалась компания Samsung, был украден исходный код Samsung Galaxy. Также были взломаны такие известные компании, как Okta, Microsoft, Cisco, AMD, Cloudflare, Twilio, LastPass.

В результате атаки на Nvidia был украден 1 ТБ данных, в том числе исходный код драйверов видеокарт. Позже через открытый чат Lapsus$ стали предлагать свой инструмент для майнинга на графических процессорах компании, позволяющий обходить внутренние ограничения. В дальнейшем украденные сертификаты Nvidia использовались злоумышленниками для подписи своего ВПО, чтобы создавать видимость легитимной программы: сертификаты использовались для подписи Cobalt Strike beacons и Mimikatz, а также различных бэкдоров и троянов удаленного доступа.

Еще одним громким инцидентом стала атака на компанию Okta, которая разрабатывает решения для управления учетными записями и доступом, в том числе решения для многофакторной аутентификации. По утверждениям злоумышленников, их интересовали клиенты компании (атака затронула около 2,5% клиентов). К слову, сама Okta была взломана в результате компрометации своего подрядчика. Практически с одинаковой частотой в атаках на IT-компании использовались приемы социальной инженерии, компрометация учетных данных и эксплуатация уязвимостей на периметре. В каждой третьей атаке были замечены программы-шифровальщики.

Прогнозы на 2023: атак меньше не станет

Атаки на цепочки поставок ПО и услуг будут продолжаться, а значит, злоумышленники продолжат взламывать инфраструктуру IT-компаний. Поэтому необходимо предусмотреть меры защиты против таких событий, как, кража сертификатов, утечка и модификация исходного кода программных продуктов, распространение вредоносных обновлений, несанкционированный доступ к данным или инфраструктуре клиентов. Поставщики облачных сервисов все чаще будут подвергаться атакам злоумышленников, по мере того как компании переносят свои данные в облачную инфраструктуру. В основном стоит ожидать атак, направленных на компрометацию учетных данных для доступа к ресурсам.

[1] Общемировые данные, основанные на собственной экспертизе компании, результатах расследований, а также на данных авторитетных источников.

Наука и образование страдают от шифровальщиков

Учреждения из сферы науки и образования входят в топ самых часто атакуемых организаций. Количество атак на них сопоставимо с результатами 2021 года[1]. Более чем в половине случаев злоумышленники смогли украсть конфиденциальные данные, преимущественно персональные данные пользователей. В каждой второй атаке использовались шифровальщики, а основной целью злоумышленников было получение выкупа от образовательного учреждения.

В 59% случаев злоумышленники прибегали к методам социальной инженерии в адрес сотрудников, а в 25% атак для доступа к ресурсам организации подбирали учетные данные или использовали скомпрометированные пароли. В каждой пятой атаке злоумышленники эксплуатировали уязвимости в ПО. За 2022 год увеличилась доля атак на веб-ресурсы: с 11% до 20%.

Прогнозы на 2023

В атаках на научные и образовательные учреждения злоумышленники будут преследовать разные цели. Некоторые группировки, атакующие научно-исследовательские центры, будут охотиться за исследовательскими наработками, другие — за персональными и учетными данными, которые можно продать или переиспользовать в других атаках. Вымогатели-шифровальщики тоже продолжат атаки на эти организации.

Стоит ожидать развития атак на сервисы онлайн-обучения. Помимо пользовательских данных, здесь представляют ценность и сами обучающие материалы: доступ к дорогостоящим курсам можно продать по более низкой стоимости. В таких системах в случае их компрометации под угрозой могут оказаться и платежные данные, например в случае внедрения вредоносных скриптов на сайт. Кроме того, образовательные платформы могут служить для распространения вредоносного ПО и проведения атак на пользователей.

Атаки на пользователей: 2022 год запомнился масштабными утечками данных

Количество атак на частных лиц увеличилось на 44%. На обычных пользователей пришлось 17% от числа всех атак[2]. Традиционно основной вектор атаки — это различные приемы социальной инженерии, которые использовались в 93% случаев. Для организации таких атак злоумышленники создавали фишинговые сайты (56%), отправляли вредоносные письма по электронной почте (39%), искали жертв в социальных сетях (21%) и мессенджерах (18%).

В 64% атак злоумышленникам удавалось украсть данные. В основном это были учетные данные (41% среди украденной информации), персональные (28%) и платежные (15%). Пользователи также стали жертвами множества утечек данных, которые произошли в крупных компаниях и популярных сервисах, в числе которых Яндекс.Еда, «ВкусВилл», Whoosh, «СДЭК», Delivery Club, «Гемотест», DNS.

[1] Общемировые данные, основанные на собственной экспертизе компании, результатах расследований, а также на данных авторитетных источников.
[2] Общемировые данные, основанные на собственной экспертизе компании, результатах расследований, а также на данных авторитетных источников.

Злоумышленники смогут агрегировать утекшие данные для того, чтобы получить более полную информацию о конкретных пользователях, использовать их в новых атаках. По данным РКН, с начала года произошло не менее 60 крупных утечек персональных данных, содержащих более 230 млн записей с личной информацией граждан.

В начале года мы прогнозировали распространение модели «фишинг как услуга» и к концу года зафиксировали усиление этого тренда. В III квартале 2022 года число массовых кампаний с использованием социальной инженерии увеличилось на 34% в атаках на частных лиц по сравнению со II кварталом. Преимущественно такой рост вызван активным использованием фишинговых комплектов — готового набора программ для проведения фишинговой атаки, в который могут входить готовые фишинговые страницы и формы ввода данных, скрипты для рассылки сообщений жертвам и скрипты для отправки украденных данных злоумышленникам.

В каждой второй атаке на устройства пользователей загружались вредоносные программы. В 2022 году доля использования шпионского ПО в атаках на частных лиц выросла на 12 п. п. и составила 42%. Количество атак с использованием банковских троянов почти не изменилось, но в процентном соотношении их доля составляет 23%, что несколько меньше, чем в прошлом году. Сайты все чаще становятся источником заражения вредоносным ПО — 40% случаев против 29% в 2021 году. С ростом удаленной занятости и использования личных устройств в рабочих целях атаки на частных лиц могут приводить к компрометации корпоративных систем.

Прогнозы на 2023: рост числа взломов аккаунтов в популярных мессенджерах и соцсетях

В 2022 году пользователи стали жертвами масштабных утечек данных, что позволит злоумышленникам совершенствовать схемы атак с использованием социальной инженерии, проводить атаки более точечно, располагая детальной информацией о действиях жертвы в скомпрометированных сервисах. Традиционно мы рекомендуем соблюдать особую бдительность в период распродаж, с осторожностью относиться к любым предложениям, связанным со значимыми общественными и культурными событиями, премьерами фильмов и сериалов, спортивными событиями. Распространение готовых комплектов для проведения массовых фишинговых атак еще больше увеличит активность злоумышленников в отношении частных лиц, особенно в отношении клиентов онлайн-банков и других онлайн-сервисов.

Мы прогнозируем увеличения числа атак на пользователей в социальных сетях и мессенджерах: взлом аккаунтов, распространение поддельных каналов и групп известных банков, магазинов и других компаний, а также известных личностей. В конце 2022 года мы уже видели волну атак, направленных на взлом аккаунтов в мессенджерах, и отметили их эффективность: пользователи оказались не готовы к новым схемам атак и легко становились жертвами злоумышленников.

В 2022 году увеличилась доля атак, в ходе которых были украдены учетные данные. Однако для входа во многие сервисы необходим второй фактор аутентификации. Сейчас мы видим, что учащаются атаки на второй фактор, и в ближайшее время таких атак будет больше. В них будут использоваться как фишинговые инструменты, социальная инженерия, так и вредоносные программы с функциями кражи SMS и пуш-уведомлений.

Безопасность операционных систем:
обзор тенденций и прогнозы на 2023 год

Александр Попов, главный исследователь безопасности открытых операционных систем, Positive Technologies

В сложных системах невозможно совершить прорыв и резко «включить» безопасность. Необходима комплексная работа сразу по множеству направлений. И в 2022 году в мире разработки операционных систем продолжалось планомерное повышение уровня безопасности.

Среди важных событий стоит отметить:

- совершенствование средств фаззинга для поиска уязвимостей,
- работы по защищенным ядерным аллокаторам для Linux и XNU в iOS 15,
- продолжение интеграции ОС с аппаратными механизмами безопасности,
- внедрение поддержки языка программирования Rust в ядро Linux 6.1, что позволит писать код с меньшим количеством уязвимостей.

Работа по этим направлениям продолжится в 2023 году, и мы в Positive Technologies внимательно следим ней и тоже проводим исследования.

В России в 2022 году особое внимание уделялось вопросам независимости и безопасности Linux-систем, поскольку западные производители ОС ушли с российского рынка. Без защищенности операционной системы невозможно выстроить безопасность информационной системы в целом.
Кроме того, по нашим данным, доля атак на Linux-системы в III квартале 2022 года выросла до 30% от всех атак с использованием вредоносного ПО. Для GNU/Linux появляются новые шифровальщики, руткиты со средствами удаленного управления, шпионское ПО, майнеры.

Поэтому перед разработчиками отечественных дистрибутивов GNU/Linux стоят важнейшие задачи: включение средств самозащиты ядра, повышение безопасности параметров по умолчанию, контроль цепочки поставки ПО и оперативный выпуск обновлений безопасности. Без этого невозможно противодействовать эксплойтам для уязвимостей ОС и распространению вредоносного ПО.

При этом у эксплуатантов есть свои не менее сложные вызовы: им нужно настроить весь парк своих информационных систем по лучшим практикам безопасности Linux, так как риски сегодня очень велики. Более того, средства защиты и параметры ОС нужно выбирать с учетом модели угроз информационной системы. Это большой фронт работ для отечественной IT-отрасли на 2023 год, и мы в Positive Technologies внесем свой вклад в это важное дело.

Безопасность мобильных приложений и устройств:

брешей становится меньше, а специалистов по анализу защищенности по-прежнему не хватает

Артем Кулаков, старший специалист группы исследований безопасности мобильных приложений, Positive Technologies

И снова небезопасное хранение данных

За 2022 год наша команда обнаружила 216 уязвимостей в 25 парах исследованных приложений для платформ Android и iOS. Наибольшая доля уязвимостей (14%) пришлась на хранение пользовательских данных в открытом виде. Несмотря на усилия со стороны разработчиков операционных систем и сообществ по безопасной разработке приложений, этот класс уязвимостей продолжает уверенно сохранять лидерство несколько лет подряд. Этот тренд сохранит актуальность в 2023 году, хотя использовать криптографию в мобильных приложениях сегодня очень просто: и вендорские, и опенсорсные решения облегчают разработчикам работу с криптографическими примитивами.

Второе место поделили между собой уязвимости, касающиеся контроля целостности приложений и хранения конфиденциальной информации в коде (по 9% на каждый класс). Замыкает тройку лидеров класс уязвимостей, связанных с проверками на недоверенное окружение (8%). Наличие в приложениях вышеперечисленных уязвимостей свидетельствует о том, что разработчики недостаточно строго контролируют целостность приложений и среды их выполнения. Если добавить к этому отсутствие хорошей обфускации кода (такую комбинацию мы обнаружили в 36% приложений, исследованных в 2022 году), складывается благоприятная ситуация для злоумышленников: становится очень просто проводить качественный анализ приложений, что, в свою очередь, упрощает создание ботов, клонов и троянов, нацеленных на конкретные приложения.

Количество уязвимостей пошло на спад

Самым любопытным трендом 2022 года стало отсутствие в приложениях некоторых классов уязвимостей. Например, разработчики теперь не хранят криптографические ключи в файловой системе и не допускают ошибки, открывающие возможность обхода директорий (path traversal). Уязвимость, связанная с небезопасной отправкой неявных межпроцессных сообщений, встретилась нам в исследованных приложениях в 2022 году всего лишь раз (в предыдущем году — шесть случаев). Это связано с тем, что разработчики стали чаще следовать хорошим архитектурным практикам. Это позволило существенно уменьшить поверхность атаки на приложения и даже полностью нивелировать некоторые типы уязвимостей. Например, в Android-приложениях, использующих подход single activity, есть всего одна активность, что значительно снижает количество возможных точек входа. За счет этого разработчикам становится проще контролировать точки входа в приложение и защищать их. Мы ожидаем, что эта позитивная тенденция будет набирать обороты в 2023 году.

Новые версии операционных систем тоже помогают разработчикам приложений: вводятся более гранулярные разрешения на выполнение системных операций, а для ряда разрешений появилась возможность запрашивать их каждый раз. К примеру, теперь не нужно навсегда выдавать приложению разрешение на доступ к геолокации.

Поддельные приложения — бич 2022–2023 годов

2022 год вывел проблему клонированных и поддельных приложений на новый уровень. Мобильные приложения многих компаний были удалены из официальных магазинов, из-за чего пользователям пришлось искать их на других площадках. Злоумышленники не преминули этим воспользоваться и стали активно размещать фальшивые приложения известных компаний. Еще один интересный момент: чтобы установить на смартфон приложение из стороннего источника, необходимо включить соответствующую функцию (по умолчанию загрузка приложений не из официальных магазинов запрещена разработчиками Android и iOS). Ранее злоумышленники обманом заставляли пользователей активировать эту функцию, сейчас пользователи вынуждены сами идти на это. Причем устанавливая приложение из неизвестного источника, они чаще всего не могут быть точно уверены, что оно оригинальное. К примеру, приложение, казалось бы, известного банка может быть модифицировано киберпреступниками и похищать пароль к личному кабинету. Ситуацию усугубили и сами разработчики мобильных приложений, когда начали размещать в официальных магазинах свои приложения под новыми названиями и от лица других компаний. С этого момента понять, какое приложение легитимное, а какое нет, стало еще труднее. На наш взгляд, создание поддельных приложений продолжит оставаться одной из главных киберугроз в 2023 году.

Отечественные магазины приложений выходят на арену

Запуск российских магазинов приложений, призванных заместить Google Play и App Store, — еще один вынужденный тренд 2022 года. Им предстоит пройти непростой путь, чтобы привлечь пользователей и завоевать их доверие. Помочь в этом может участие в программах bug bounty и сотрудничество с сообществами специалистов по ИБ. Основная проблема отечественных магазинов в том, что они по сути являются обычными пользовательскими приложениями и не имеют особых прав в системе. Вследствие этого требуется давать все то же разрешение на установку приложения из недоверенных источников. На наш взгляд, решить эту проблему могло бы сотрудничество разработчиков отечественных магазинов и вендоров операционных систем. Возможно, уже в 2023 году появятся первые интеграции с китайскими вендорами. Другой вариант решения проблемы — создание отечественной операционной системы, где такие магазины приложений устанавливались бы по умолчанию как системные.

Уязвимости в мобильных приложениях пора систематизировать

Мировые тренды уязвимостей в мобильных приложениях продолжают удивлять год от года: целочисленное переполнение в WhatsApp (CVE-2022-36934, CVE-2022-27492), полный захват учетной записи в TikTok через deeplink (CVE-2022-28799) и похожая проблема с обработкой ссылок в Zoom (CVE-2022-28763). Кроме того, исследователям удалось взломать Tesla, выполнив MITM-атаку на BLE-соединение (bluetooth low energy) между автомобилем и мобильным приложением (CVE-2022-37709). Перечисленные инциденты — лишь малая часть того, о чем стало публично известно в 2022 году. Стоит отметить, что это не новые виды атак или неизвестные эксплойты, а типовые уязвимости, которые мы каждый год видим в приложениях. Отсюда напрашивается вывод: разработчики не учатся на своих ошибках. Почему? Возможно, не хватает инструментов. Так, например, мировое сообщество по ИБ уделяет теме классификации уязвимостей в мобильных приложениях очень мало внимания. OWASP Mobile Top 10 — рейтинг наиболее часто встречающихся угроз — не обновлялся с 2016 года, тогда как OWASP Top 10 для веб-угроз был актуализирован в 2021 году.

Первые три позиции в рейтинге уязвимостей мобильных приложений занимают «Неправильное использование платформы» (Improper Platform Usage), «Небезопасное хранение данных» (Insecure Data Storage), «Небезопасные коммуникации» (Insecure Communication), что отличается от наших результатов исследований безопасности приложений в 2021 и 2022 годах. Более актуальный стандарт — OWASP Mobile Application Security Verification Standard (MASVS) — составлен с позиции проверки приложения разработчиком, а не атакующим. В связи с этим назрела острая необходимость в составлении классификации уязвимостей для мобильных приложений, аналогичной той, что уже существует для веб-приложений.

В 2023 году не потеряет актуальности проблема нехватки специалистов по анализу защищенности мобильных приложений. В то же время развитие тематических сообществ, программ bug bounty, в том числе российских, и появление более продвинутого инструментария дадут толчок к увеличению числа специалистов этого профиля на рынке, а значит, и к повышению уровня безопасности мобильных приложений.

Искусственный интеллект и безопасность: чем запомнился 2022 год и чего ждать в 2023-м

Александра Мурзина, руководитель отдела перспективных технологий, Positive Technologies

Главной темой 2022 года был расширяющийся ландшафт киберугроз от применения ИИ: от кражи данных до эксплуатации уязвимостей инфраструктуры. При этом начало года не принесло новых сюрпризов от технологий. В классической безопасности все большее внимание уделяется направлениям DevSecOps. Умные технологии тоже не отстают, и сейчас начинает серьезно развиваться направление MLDevSecOps. Если в предыдущие годы мы видели лишь концепты, то сегодня многие из них превратились в полноценные фреймворки, готовые к внедрению в жизнь. Летом аналитическое агентство Gartner выпустило исследование об уровне внедрения ИИ и сопутствующих рисках безопасности. По результатам опроса оказалось, что 41% компаний столкнулись с нарушениями конфиденциальности ИИ или инцидентами безопасности. Из этих инцидентов 60% были компрометацией данных внутренними злоумышленниками, а 27% — злонамеренными атаками на инфраструктуру ИИ. При этом аналитики Gartner подчеркивают, что в настоящее время есть значительное расхождение между тем, что́ директора по информационной безопасности и разработчики решений ИИ считают существенным риском. Например, CISO уверены, что риск ИИ материализуется лишь в 26% случаев, тогда как специалисты, которые разрабатывают ИИ, заявляют о 54%-ной вероятности. Gartner рекомендует руководителям компаний подготовиться к такому развитию событий, внедрив модель управления доверительными рисками и безопасностью ИИ (AI TRiSM). Она позволит обеспечить надежность, достоверность, безопасность и конфиденциальность моделей ИИ.

Вредоносный ИИ и другие инциденты

Без громких инцидентов в 2022 году тоже не обошлось. Например, на основе доступных в Сети видео мошенники создали дипфейк Патрика Хиллмана, директора по коммуникациям криптовалютной биржи Binance, и использовали его в серии видеозвонков с представителями различных криптопроектов. Неожиданно Патрик стал получать сообщения с благодарностью за проведенные встречи, на которых он даже не присутствовал.

В части применения ИИ для атак много исследований было посвящено тому, что сами модели машинного обучения могут быть вредоносным ПО. В частности, было организовано несколько открытых конкурсов, один из которых прошел на крупной конференции по машинному обучению — NeurIPS 2022. На ней участникам предлагали научиться прятать вредоносный код в весах моделей и выявлять подобные случаи.

Как скоро ИИ заменит художников и писателей?

В развитии технологий машинного обучения в 2022 году можно выделить два ярких направления: генерацию изображений по описанию и написание текстов чат-ботом ChatGPT компании OpenAI.
Технология генерации картин развивается уже достаточно давно. Например, еще в прошлом году OpenAI поделилась своим исследованием нейросети DALL-E. На тот момент технология была закрытой (было доступно только демо). Технические энтузиасты на открытых датасетах обучили модели и выложили в опенсорс нейросети Stable Diffusion и MidJourney. На их основе другие энтузиасты стали создавать небольшие сервисы, тем самым популяризируя эту технологию.

Вопросы безопасности в данном случае касаются преимущественно приложений, в которые встраиваются данные технологии, так как сам факт генерации изображений (даже на основе реальных фотографий пользователей) не несет особой угрозы. Однако не стоит забывать о дополнительном программном обеспечении, которое, возможно, потребуется установить, — оно может быть небезопасным.

В 2022 году никто в ИТ и ИБ не ожидал столь радикального прорыва от ChatGPT, текстового чат-бота, основанного на GPT-3 — большой языковой модели. Уже с 2020 года модель GPT-3 умела генерировать тексты, отвечать на вопросы и быть чат-ботом. Компания OpenAI серьезно дообучила ее, сделав акцент именно на диалогах, и в ноябре 2022 года представила ChatGPT. В настоящее время она умеет писать код и проверять его на ошибки, искать баги и уязвимости, а также создавать к ним эксплойты. Однако стоит отметить, что ChatGPT не всегда справляется идеально, и даже ее создатели призывают пользоваться технологией с осторожностью и не верить безоговорочно тому, что она выдает. Все-таки модель обучена на данных из интернета, где можно найти подтверждение любой точки зрения, а значит, корректность текста, создаваемого ChatGPT, остается под большим вопросом.

Прогнозы на 2023: создание коммерческих решений ИИ на базе опенсорсных моделей

Можно ожидать, что на основе ChatGPT и технологии, создающей изображения по описанию, в 2023 году создадут интересные приложения, которые изменят целые индустрии. Однако люди опасаются, что ИИ может заменить труд некоторых специалистов и автоматизировать многие процессы в различных отраслях экономики. Так, в 2022-м в Сети распространялись онлайн-протесты NoAIArt (#noaiart), где художники призывали запретить использование технологии, генерирующей изображения по текстовому описанию.

Доступ к моделям машинного обучения таких компаний, как OpenAI, обычно платный, и получить его может не каждый желающий. Случаи с Stable Diffusion и MidJourney показали, что есть техноэнтузиасты, готовые за свои деньги обучать большие модели и выкладывать их в опенсорс. Мы предполагаем, что в 2023-м этот тренд усилится и специалисты по ИИ будут разрабатывать коммерческие решения на базе опенсорсных моделей.

Кроме того, ожидается, что в России и мире ужесточится регулирование в области применения алгоритмов машинного обучения, основанных на чувствительных данных, поскольку утечка такой информации или ошибка самой модели могут привести к серьезным последствиям.

Крипта, блокчейн, метавселенные и не только


Игорь Агиевич и Андрей Бачурин, специалисты по безопасности распределенных реестров, Positive Technologies

Актуальные векторы атак

2022 год, по данным Glassnode, побил все рекорды по количеству взломанных криптопроектов и похищенных средств: ущерб составил более 3 млрд долларов. В первую очередь год запомнился атаками на блокчейн-мосты. Самыми прибыльными для киберпреступников оказались взломы BSC Token Hub, принадлежащего крупнейшей криптовалютной бирже в мире Binance (украдено 566 млн долларов), Ronin (552 млн долларов), Wormhole (326 млн долларов) и Nomad (190 млн долларов). Кроме того, зафиксирован первый случай успешного взлома криптомата. Атаку провели через интернет: злоумышленники проэксплуатировали уязвимость нулевого дня в устройствах GENERAL BYTES — второго по величине производителя криптоматов в мире. Можно предположить, что криптовалютные банкоматы станут мишенью для киберпреступников в 2023 году.

Растет интерес злоумышленников к криптобиржам и DeFi-протоколам: количество атак на блокчейн-проекты в два раза превысило число атак за 2021 год[1]. Широкое распространение получило мошенничество с эрдропами (airdrop): на электронную почту отправлялись фейковые сообщения о бесплатной раздаче криптовалют, токенов или NFT. Дарение активов за выполнение пользователями определенных действий действительно популярно у криптовалютных стартапов в момент запуска. Злоумышленники, как и всегда, используют актуальную тему в своих целях. Под видом бесплатных NFT-токенов и виртуальных коллекционных предметов они также рассылают вредоносное ПО.

[1] Общемировые данные, основанные на собственной экспертизе компании, результатах расследований, а также на данных авторитетных источников.

В 2022 году явным трендом был вектор атаки, связанный с перенаправлением пользователей на подконтрольный злоумышленнику сервер при переходе на легитимный сайт проекта. При этом даже сертификат доменного имени браузером помечался как легитимный. Пострадали как минимум: Convex Finance, Allbridge, Ribbon Finance, DeFi Saver, Celer Network, Mad Meerkat finance. Причина заключалась в том, что злоумышленник смог получить доступ к DNS-записям у регистратора DNS и указать подконтрольные IP-адреса, ассоциированные с доменными именами пострадавших проектов. Исключение — случай с Celer Network, когда киберпреступник провел атаку BGP hijacking: поменялся не IP-адрес, а маршрут к нему, что, по сути, привело к такому же результату — перенаправлению пользователя на подконтрольный злоумышленнику сервер. Каким бы ни был конкретный вариант атаки, во всех случаях итог был один: обманывали не только пользователей, но и центры выдачи сертификатов. Через эти центры злоумышленники выпускали доверенные сертификаты для HTTPS, чтобы не выдавать браузерам жертв предупреждения о недоверенном соединении. Примечательно, что даже когда проект узнавал об атаке, выпущенные злоумышленником сертификаты не отзывались. Это позволяло атакам развиваться еще некоторое время, пока данные о DNS-записях не обновились в DNS-кэше на устройствах пользователей.

Еще один любопытный момент: старый добрый фишинг успешно срабатывает при атаках не только на простых граждан, которых в силу доверчивости и слабого знакомства с криптотехнологиями очень легко обмануть, но и на разработчиков. Излюбленный злоумышленниками метод социальной инженерии помогает получить приватные ключи, которые позволяют распоряжаться криптотокенами. В целом разработчики DeFi-платформ сегодня являются объектами повышенного внимания киберпреступников (в особенности группировок, чьей квалификации достаточно, чтобы разобраться в работе кода) из-за того, что имеют непосредственный доступ к коду площадки и ее инфраструктуре. Хороший пример в 2022 году — фишинговая почтовая рассылка работникам deBridge якобы от ключевого сотрудника этой организации. Как видно, далеко не все компании следуют примеру Positive Technologies и проводят киберучения с фишинговыми рассылками, а также помечают письма, которые пытаются мимикрировать под доверенный источник.

Есть и хорошие новости

Если говорить о позитивных трендах, то в 2022 году по-прежнему наблюдалась устойчивая тенденция проводить аудит смарт-контрактов. В мире продолжают появляться компании, специализирующиеся на проверке безопасности кода смарт-контрактов, расположенного в блокчейне, однако пока их недостаточно для покрытия всех запросов. Кроме того, в этой области наблюдается дефицит кадров: специализированных курсов не так много. В основном они охватывают только язык Solidity (для EVM-подобных блокчейнов вроде Ethereum), тогда как все большую популярность приобретают языки программирования Rust (смарт-контракты для Solana, NEAR) и Go (на нем написана часть кода, используемого в различных блокчейнах и протоколах для работы с ними).

Активно развивается направление bug bounty: в настоящее время сервис Immunefi, аналог HackerOne для блокчейна, — одна из немногих площадок, помогающая компаниям найти уязвимости, ускользнувшие от аудиторов, причем не только на уровне смарт-контрактов и криптовалюты, а несколько шире. Например, выплачивают вознаграждения за бреши в защите на стороне сайтов — их аудиторские фирмы в принципе не проверяют. Возможность изменения кода сайта, как правило, приводит к подмене адреса кошелька получателя. В итоге пользователь теряет свои деньги. Несмотря на отсутствие прямой потери средств самого криптопроекта от таких атак, сложилась практика возмещения ущерба пользователям для уменьшения репутационных издержек. Таким образом, зачастую уязвимости выявляются не на уровне блокчейна, а на уровне его узлов, в инфраструктуре, на сайте, сервере приложений, на уровне баз данных (если используются). Поэтому аудит безопасности проектов может и должен быть шире, чем только аудит смарт-контрактов. Bug bounty — один из способов расширить его охват.

Иногда проблемы безопасности возникают по вине администратора проанализированного проекта, и при аудите их обнаружить невозможно.

Например, аудиторы могут посчитать необходимым изменить код так, чтобы важная функция выполнялась только после нескольких подписей разных администраторов (это важно для защиты от утечки приватного ключа у одного человека). При этом код действительно изменится в соответствии с требованиями проверяющих, но администратор вместо использования публичных ключей разных пользователей может создать себе несколько ключей. Таким образом, угроза утечки сохранится, что аудиторы не способны заметить.

Интересный случай произошел под занавес 2022 года с проектом Rubic. По ошибке в список криптобирж был внесен адрес криптовалюты. Особенность кода криптопроекта позволила атакующему этим воспользоваться. В момент аудита кода список был пуст, и аудиторы не могли спрогнозировать возникновение такой ситуации.

Уязвимости на уровне протоколов в 2022 году приводили или могли привести к проблемам на уровне самой блокчейн-сети. С этим столкнулись Avalanche, Lightning Network, Zcash.

Массовое принятие криптовалюты

Количество пользователей криптовалют по всему миру продолжает увеличиваться. Например, в России рост интереса к криптовалюте вызван миграцией граждан, ограничениями Центробанка на перевод денежных средств и вывоз наличной валюты за рубеж. Не последнюю роль в том, что россияне начали активно пользоваться криптовалютой для международных переводов, сыграло большое количество криптоматов в странах ближнего зарубежья. В 2023 году тенденция на массовое принятие криптовалюты усилится.

Отличие подходов к регулированию криптовалюты в России и мире

Остро стоит вопрос регулирования криптовалюты. По данным отчета Huobi, в 2022 году власти 42 стран выпустили более ста мер регулирования и руководящих указаний для участников криптоиндустрии. В ближайшее время в США и странах ЕС намерены запретить анонимные транзакции, из-за чего, кстати, блокчейн может потерять свою особенность и главное преимущество — отсутствие прямой связи между конкретным пользователем и адресом кошелька.

Например, в сентябре 2022 года Минфин США ввел санкции в отношении Tornado Cash — децентрализованного протокола для проведения анонимных операций. В США также набирает обороты «зеленая повестка»: законотворцы пытаются оценить вред, причиняемый экологии майнингом. Некоторые штаты стараются урегулировать майнинг самостоятельно. В России в ноябре 2022 года в Госдуму внесен законопроект о легализации майнинга криптовалюты. Кроме того, отечественным компаниям планируют разрешить рассчитываться в цифровой валюте с зарубежными партнерами. Однако ждать легализации криптовалюты в качестве платежного средства для физических лиц в скором времени, на наш взгляд, не стоит. Это подтверждается переносом срока рассмотрения законопроекта на 2023 год из-за необходимости дополнительных согласований.

Прогнозы на 2023: децентрализованные биржи на мушке

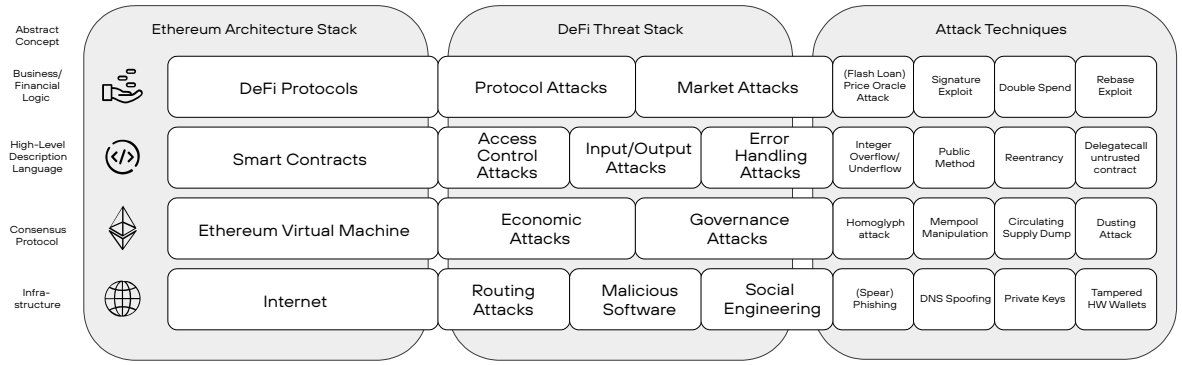
Все больше компаний строят свои цифровые территории, а значит, метавселенные, о которых мы говорили еще в 2022-м, в ближайшие годы получат новый виток развития. Вместе с их расцветом возрастет и популярность NFT, так как эти технологии взаимовыгодно существуют друг с другом. В одних случаях это выставка картин в диджитал-пространстве (вполне вероятно, полностью виртуальном), в других — NFT-картина может быть артефактом, используемым в различных играх.

Блокчейн-площадки быстро привлекают новых пользователей. Среди них много любителей онлайн-игр, которым, как правило, интересны GameFi-проекты. Такие программы позволяют зарабатывать, играя. Еще один тренд, который станет более явным в 2023 году, — learn to earn (учись, зарабатывая): это способ получить криптовалюту в процессе изучения чего-либо, например иностранных языков. Развитие learn to earn обусловлено тем, что после пандемии онлайн-обучение стало неотъемлемой частью современной жизни.

Высокая стоимость энергоресурсов в некоторых частях света уже привела к массовой миграции майнинговых компаний в страны с более низкими ценами на электричество, в первую очередь Россию и Казахстан (эта тенденция продолжится, чему также поспособствует регулирование майнинга), или может стать причиной их закрытия. Некоторые крупные майнинговые фирмы в США уже столкнулись с угрозой банкротства. То же самое может произойти в Европе.

Мы ожидаем, что в 2023 году участятся случаи взлома децентрализованных бирж[1]. Недавний крах биржи FTX, второй по величине в мире, стал причиной значительного оттока пользователей с других централизованных платформ[2], например Binance. Криптовалюту активно переводят на DeFi-платформы, где пользователи могут обменивать токены напрямую, используя ликвидность децентрализованной криптобиржи. А злоумышленники, как известно, всегда следуют за потенциальными жертвами и деньгами.

Можно предполагать, что тренд на использование способов проникновения в систему, не покрываемых аудитом смарт-контрактов, сохранится. На рисунке представлено, сколько векторов атаки остается после проверки аудиторами: в лучшем случае она охватывает три первые строчки, а последней вовсе не уделяют внимания.



[1] Децентрализованные биржи (DEX) не имеют единого органа управления как такового. Они не хранят денежные средства и персональные данные пользователей на своих серверах и выступают только платформой для поиска совпадений по заявкам на покупку или продажу активов.

[2] Централизованные биржи (CEX) – это традиционные биржи, имеющие руководство, которое несет ответственность за конфиденциальные данные пользователей, хранит историю торгов, контролирует работу биржи и единолично принимает все решения о развитии проекта.

Заключение

Современные реалии повысили актуальность и важность обеспечения информационной безопасности и киберустойчивости компаний, государственных структур и отраслей экономики. Сегодня внимание государства к ИБ многократно возрастает. Например, майский указ Президента РФ № 250 направлен на радикальное повышение защищенности от кибератак ключевых предприятий страны. Под действие этого указа попал более широкий круг организаций, чем, например, под действие 187-ФЗ о КИИ, а в вопросы обеспечения ИБ теперь вовлекаются первые лица компаний.

В 2023 году стоит ожидать более плотной работы регуляторов по ужесточению ответственности компаний за утечки персональных данных (в частности речь идет о вводе оборотных штрафов), а также повышения требований к обеспечению ИБ, вывода вопроса кибербезопасности на уровень отраслевых ведомств. Учитывая то, что кибератака может нанести серьезный ущерб не только отдельной организации, но и целым отраслям, подобные инициативы регуляторов действительно актуальны.
В ушедшем году появилось много новых, ранее неизвестных APT-группировок, которые стремились нанести бизнесу репутационный ущерб. В 2023-м эта тенденция сохранится.

Острая необходимость в практической ИБ определяет запрос к российским вендорам на качественные и практически применимые технологии в области ИБ. Наряду с историческим кадровым голодом в области кибербезопасности это будет стимулировать развитие рынка MSSP, а также создавать запрос на технологии с высокой автоматизацией противодействия киберугрозам. Так, задачи по обнаружению кибератак и реагированию на них будут преимущественно ложиться не на плечи операторов продуктов ИБ, а на искусственный интеллект.

Один из главных трендов — активный переход российских компаний на отечественные операционные системы. Мы прогнозируем увеличение числа кросс-платформенных хакерских инструментов, в том числе разработанных или переписанных под Linux.

Нехватка кадров, рост числа атак, в том числе целенаправленных, недостатки решений ИБ, уход зарубежных вендоров, множественные утечки данных, увеличение количества уязвимостей — все это заставляет российские компании (да и не только российские) менять парадигму обеспечения кибербезопасности в пользу обеспечения цифровой устойчивости предприятия. Что важно, ее необходимо обеспечивать точечно, сфокусировавшись на самых ценных активах компании, негативное воздействие на которые может привести к наступлению недопустимых для бизнеса событий.

Для заметок


pt