Предсказания «Лаборатории Касперского» об угрозах для корпораций на 2023 год: шантаж в СМИ, фейковые утечки и атаки через облако.

Автор:
Security Services

Угрозы для корпораций: предсказания на 2023 год

kaspersky АКТИВИРУЙ БУДУЩЕЕ

«Лаборатория Касперского» расскажет о возможных угрозах 2023 года

Что грозит корпорациям в 2023 году

Каждый день «Лаборатория Касперского» обнаруживает в среднем 400 000 вредоносных файлов. В год их число достигает 144 млн. Ландшафт угроз постоянно меняется: создается новое вредоносное ПО, в том числе шпионское, появляются продвинутые методы фишинга и новые приемы социальной инженерии. СМИ регулярно сообщают о киберинцидентах и утечках данных, которые впоследствии оказываются в открытом доступе в даркнете. Из-за хакерских атак постоянно страдают люди, корпорации и целые страны, причем речь не только о финансовых потерях. В некоторых случаях кибератаки могут представлять угрозу для жизни — например, если это атаки на объекты критической инфраструктуры.

В прошедшем году безопасность информационных систем корпораций и государственных структур была как никогда значима, и в 2023-м она не станет менее важной. В рамках Kaspersky Security Bulletin команды DFI (Kaspersky Digital Footprint Intelligence) и DFIR (Digital Forensics and Incident Response) подготовили обзор угроз, которые будут актуальны для этого сегмента.

1

Будет еще больше утечек персональных данных, появятся комбинированные базы

В 2022 году тренд на утечки персональных данных демонстрировал стремительный рост. За этот год в открытом доступе оказалось более 1,5 млрд записей, содержащих персональные данные российских пользователей.

О безопасности данных

Мы регулярно наблюдаем, что для регистрации на сторонних сайтах и сервисах люди используют адрес корпоративной электронной почты, которая попадает в публичное поле в результате взломов этих сервисов. Таким образом под угрозу ставится безопасность компании — владельца этой почты: поверхность атаки в ее инфраструктуре увеличивается, поскольку возрастает количество потенциально уязвимых объектов. Появление корпоративных email-адресов в открытом доступе может вызвать интерес киберпреступников и запустить на ресурсах даркнета (форумах, каналах обмена мгновенными сообщениями, onion-ресурсах и т. д.) обсуждение атак на организацию. Кроме того, корпоративный адрес с большей вероятностью будут использовать для фишинга и социальной инженерии.

В 2023 году мрачный тренд на утечки получит новый виток: злоумышленники будут не просто «сливать» базы, но и совмещать информацию из различных источников. Так, уже в мае 2022 года появилась карта, которая объединяла данные о пользователях различных российских сервисов — «Яндекс.Еды», ГИБДД, СДЭКа, Avito, Wildberries, «Билайна» и т. д. Это наглядно демонстрирует тот факт, что киберпреступники способны объединять имеющуюся у них информацию в подробное «досье» на пользователей, что позволяет им придумывать и реализовать более продвинутые, таргетированные схемы социальной инженерии и кибершпионажа. Чтобы обезопасить бизнес или государственную структуру от подобных угроз, необходимо контролировать цифровой след компании и ее сотрудников, в том числе с помощью непрерывного мониторинга открытого интернета и даркнета.

2

Даркнет-сообщество станет еще более чутко реагировать на новостную повестку

В 2023 году рынок даркнета станет еще чувствительнее к новостной повестке: события в мире будут влиять на то, какие данные киберпреступники будут выставлять на продажу. За прошедшие два года злоумышленники в совершенстве отточили навыки адаптации и быстрого реагирования на возникающие инфоповоды. В 2022 году мы в очередной раз увидели этому подтверждение. Так, когда карты российских банков перестали работать за границей, как товар они сразу стали менее интересны не только покупателям, но и продавцам: число объявлений о продаже данных российских карт снизилось.

Для защиты от инцидентов, связанных с продажей информации, и от целевых атак на организацию в будущем году нужно не только держать руку на пульсе глобальных событий, но и следить за их последствиями в мире киберпреступников.

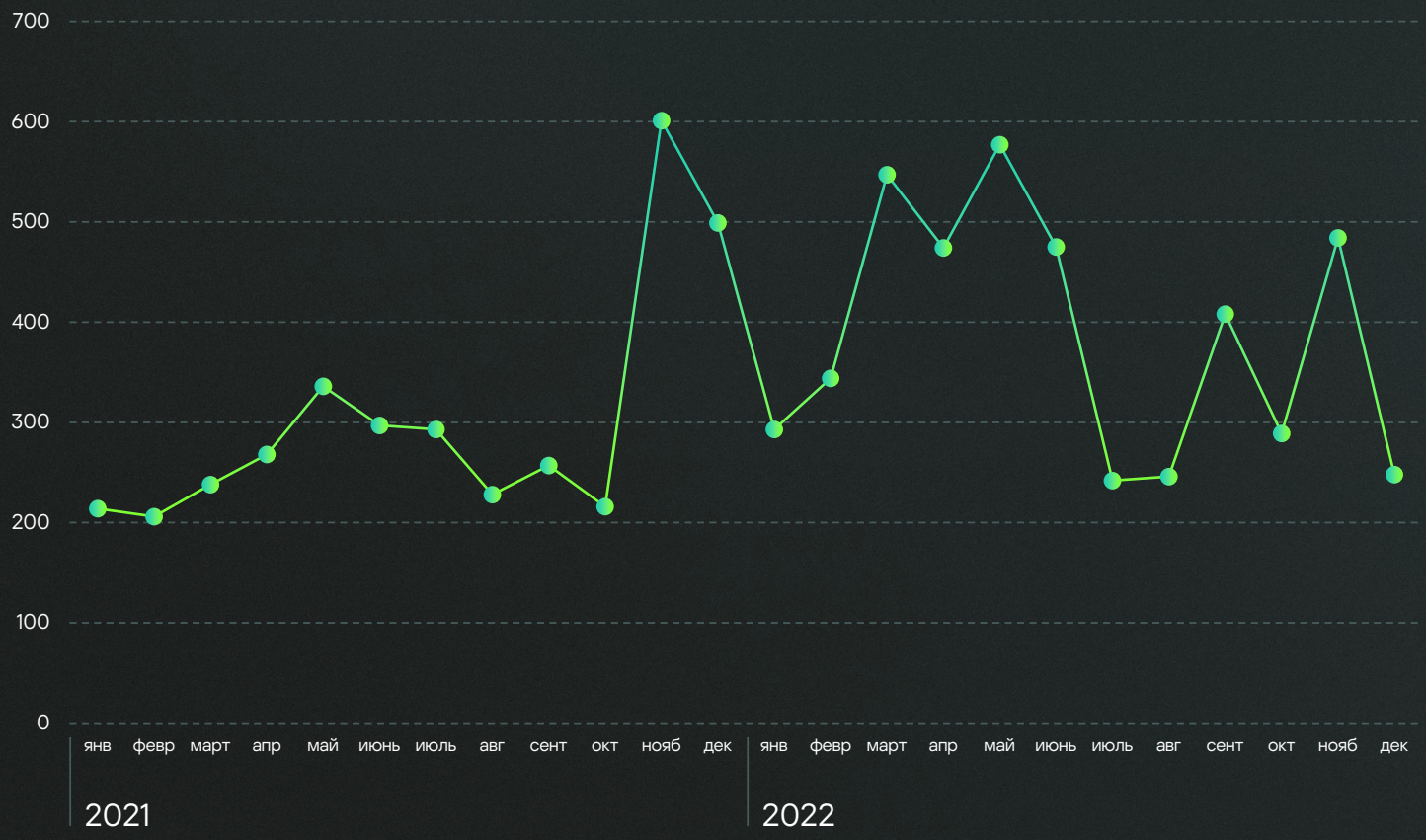
3

Шантаж в медиа: компании будут узнавать о взломе из публичных постов хакеров с обратным отсчетом до публикации данных

Разработчики вымогательского ПО создают блоги, в которых публикуют объявления о взломе компаний, а также украденные данные. В 2022 году количество публикаций в таких блогах — как на открытых ресурсах, так и в даркнете — заметно выросло. Если в течение первых 10 месяцев 2021 года мы наблюдали порядка 200-300 постов в месяц, то в конце 2021-го и первой половине 2022-го их количество на пике превышало 500 постов в месяц.

Динамика количества постов в блогах вымогателей в 2021–2022 гг., глобальная статистика

Статистика содержит данные по ресурсам, которые включены в систему мониторинга Kaspersky Digital Footprint Intelligence



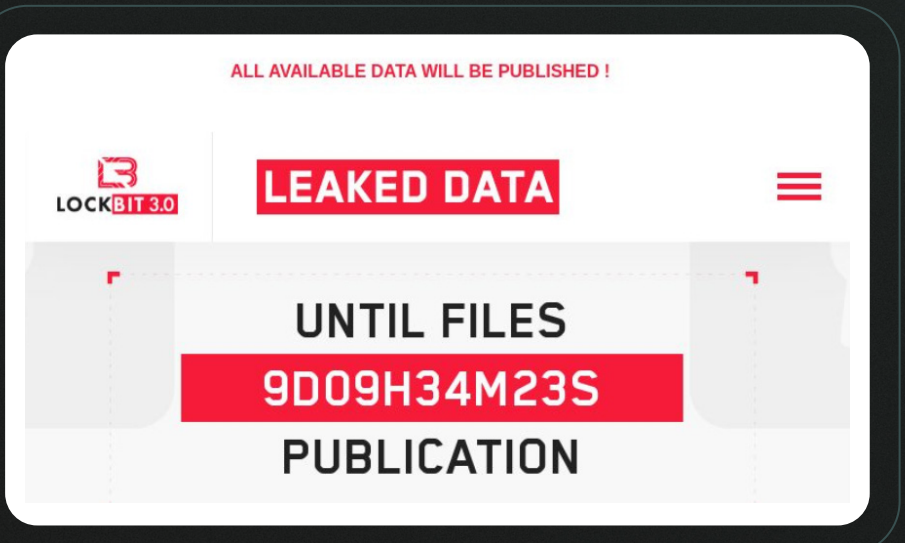
Раньше после успешной атаки вымогатели пытались договориться с пострадавшими компаниями наедине, не привлекая внимания общественности. Злоумышленники пытались оставаться невидимыми для общества, пока не получат свою выгоду, а жертвы взлома хотели исключить репутационные потери и другие последствия атаки. Теперь же киберпреступники вместо попыток связаться с компанией сразу размещают сообщение о взломе в своем блоге с обратным отсчетом до публикации утекших данных и ждут реакции жертвы. Такая схема также помогает злоумышленникам остаться в выигрыше вне зависимости от того, заплатит ли жертва выкуп. Более того, данные на продажу часто выставляются в формате аукциона, в ходе которого их стоимость может сильно вырасти и превысить сумму выкупа.

Пример объявления о взломе австралийской страховой компании Medibank, найденный с помощью сервиса Kaspersky Digital Footprint Intelligence

Подробнее о сервисе

В 2023 году мы ожидаем, что злоумышленники будут все реже пытаться установить контакт с представителями пострадавшей компании, на замену придет рост публикаций в публичном пространстве и все чаще зазвучат имена жертв в новостной ленте.

Пример обратного отсчета до публикации утекших данных в блоге шифровальщика LockBit



4

«Потехе час»: киберпреступники будут чаще публиковать фейки о взломах

Сегодня информация о новых утечках появляется почти ежедневно. Вместе с этим растет и количество фейковых сообщений. Мы полагаем, что в 2023 году злоумышленники будут чаще утверждать, что взломали ту или иную компанию, чтобы похвастаться и заработать себе репутацию. Информация об утечке, опубликованная в открытых источниках, становится инструментом манипуляции медиа, и даже без реального взлома может нанести вред целевой компании. Важно своевременно выявлять подобные сообщения и инициировать процесс по реагированию на них, схожий с реагированием на инциденты безопасности. Он включает в себя мониторинг публикаций об утечках или компрометации компании на ресурсах даркнета и теневых сайтах.

5

Популярными векторами атак станут облачные технологии и скомпрометированные данные из даркнета

К основным векторам атак — уязвимостям в публичных приложениях, скомпрометированным учетным данным и электронной почте с вредоносными ссылками и вложениями — добавятся действия и инструменты, связанные с облачными и виртуальными технологиями. Все больше компаний переносят свои информационные системы в облако, и зачастую используют для этого услуги внешних партнеров. Однако при миграции в облако информационной безопасности уделяется мало внимания: организации часто даже не ставят такой задачи перед провайдером услуг по виртуализации. А если случается инцидент, для проведения расследования не хватает данных, так как облачный провайдер не собирает и не логирует информацию о событиях в системе. Это существенно затрудняет расследование инцидента.

В 2023 году киберпреступники будут чаще покупать в даркнете доступы к уже скомпрометированным сетям разных организаций. В наших расследованиях мы наблюдаем четкую тенденцию: становится больше атак, начинающихся с использования ранее скомпрометированных учетных записей, опубликованных на теневых ресурсах. Этот тренд опасен тем, что этап компрометации учетных данных пользователей может оставаться незамеченным. Только получив ощутимый ущерб (например, столкнувшись с перебоями в работе сервиса или шифрованием данных), компания-жертва узнает об атаке.

Цифровизация повышает риски кибербезопасности. Чтобы добиться лояльности клиентов и партнеров, корпорация должна поддерживать непрерывность бизнеса и внедрять надежную защиту критически важных активов, корпоративных данных и всей IT-инфраструктуры. Зачастую в крупном бизнесе и государственных структурах такая защита многоуровневая, но даже она не исключает риск компрометации. Поэтому очень важно своевременно и правильно реагировать на инцидент и проводить расследование, чтобы устранить не только последствия, но и причину, а также не допустить повторения подобных инцидентов в будущем.

Сервис по реагированию

6

Программа-вымогатель как услуга: больше однотипных атак, сложнее инструментарий

В 2023 году модель Malware-as-a-Service продолжит набирать обороты, в частности среди вымогателей. Киберпреступники стараются оптимизировать свои трудозатраты, поэтому активно масштабируют свою деятельность и пользуются аутсорсингом, как и законный бизнес. К примеру, группа LockBit (об ее эволюции можно почитать здесь) развивает свой сервис как производитель программного обеспечения. Недавно злоумышленники даже представили собственную программу Bug Bounty. MaaS снижает порог входа в ряды киберпреступников: любой желающий может организовать кибератаку с использованием шифровальщика, взяв соответствующее вредоносное ПО напрокат.

В свою очередь, количество известных и распространенных семейств шифровальщиков будет снижаться, а атаки будут становиться все более однотипными. С одной стороны, для компаний это хорошая новость: для множества шифровальщиков будут использоваться схожие техники и тактики MaaS, а значит нужно будет учитывать меньше тактик и техник для реагирования силами SOC. При этом инструментарий атакующих будет усложняться, и только автоматизированных решений станет недостаточно для построения полноценной защиты.

Подведем итоги

Предстоящий год будет сложным с точки зрения кибербезопасности, потому что ландшафт угроз стремительно развивается. Это задает определенный темп для компаний, которые вынуждены постоянно адаптироваться к изменениям. Хорошая новость в том, что исследователи располагают продвинутыми инструментами, и могут оперативно сдерживать растущие угрозы.

Таковы наши предсказания на 2023 год. Следующей зимой мы проверим, насколько точными они оказались.

Kaspersky Digital Footprint Intelligence

Чтобы аналитики по безопасности могли оценивать угрозы со стороны внешних атакующих, быстро выявлять возможные векторы атак и принимать стратегические решения по защите от них, мы предлагаем сервис Kaspersky Digital Footprint Intelligence.

Подробнее

Kaspersky Incident Response

Если вы столкнулись с инцидентом, сервис Kaspersky Incident Response поможет предотвратить его распространение и ограничить ущерб, в частности — выявить скомпрометированные узлы и защитить инфраструктуру от подобных атак в будущем.

Подробнее

www.kaspersky.ru

#kaspersky
#bringonthefuture