Прогнозы ЛАБОРАТОРИИ КАСПЕРСКОГО на 2023 год

1. Разрушительных атак станет больше

В декабре прошлого года, вскоре после публикации наших прогнозов, стало известно об атаке CryWiper на российские государственные организации. Зловред притворялся шифровальщиком и требовал выкуп за «расшифровку» данных жертв, однако в действительности он не шифровал файлы, а целенаправленно уничтожал их.

В январе эксперты ESET обнаружили новый вайпер, который использовался для атаки на территории Украины и распространялся через групповые политики Active Directory. Этот вайпер под названием SwiftSlicer они связывают с группировкой Sandworm (она же Hades).

В июне корпорация Microsoft опубликовала доклад о группировке Cadet Blizzard, которая использовала WhisperGate и другие вайперы для проведения атак на госучреждения Украины в начале 2022 года. От ее рук пострадали не только украинские государственные учреждения, правоохранительные органы, IT-компании и аварийно-спасательные службы, но и организации в Европе, Центральной Азии и Латинской Америке.

В целом количество атак снизилось по сравнению с 2022 годом, но без масштабных инцидентов не обошлось.

Вердикт: прогноз сбылся частично ОК

2. Почтовые серверы станут приоритетной целью

В июне компания Recorded Future предупредила, что группировка BlueDelta (также известная под именами Sofacy, APT28, Fancy Bear и Sednit) эксплуатирует уязвимости почтового сервиса Roundcube Webmail для атаки на украинские организации, в том числе государственные органы и военные учреждения, обслуживающие авиационную инфраструктуру. Злоумышленники рассылали новости о российско-украинском конфликте, чтобы побудить жертву открыть вредоносное письмо и активировать эксплойт, использующий уязвимости CVE-2020-35730, CVE-2020-12641 и CVE-2021-44026. С помощью вредоносного скрипта они перенаправляли почтовые ящики жертв на подконтрольный им адрес, забирая таким образом их содержимое.

В июле мы писали о новой вариации вредоносного модуля Owowa, от которого пострадали российские пользователи. Нам удалось восстановить цепочку заражения до почтовых рассылок, похожих по стилю на ранее исследованную нами кампанию GOFFEE от группировки CloudAtlas.

В августе TeamT5 и Mandiant по итогам расследования атаки на Barracuda ESG через уязвимость CVE-2023-2868, позволяющую удаленному злоумышленнику выполнять на устройстве произвольный код, подробно описали тактики, техники и процедуры атакующих. За атакой стояла группировка UNC4841, которая использовала новые вредоносные программы для слежки за несколькими высокоприоритетными целями, чьи системы были скомпрометированы либо до, либо вскоре после выхода исправления. В частности, в арсенале

UNC4841 были бэкдоры SKIPJACK и DEPTHCHARGE и модуль запуска FOXTROT/FOXGLOVE. Злоумышленники атаковали организации из множества разных отраслей. Американское Агентство по кибербезопасности и защите инфраструктуры (CISA) опубликовало дополнительные индикаторы компрометации, связанные с эксплуатацией CVE-2023-2868.

Вердикт: прогноз сбылся ✓

3. Преемник WannaCry

К счастью, новой масштабной киберэпидемии не случилось.

Вердикт: прогноз не сбылся ✗

4. APT-группы будут атаковать спутниковое оборудование, его производителей и операторов

Единственная известная атака на спутниковые технологии за последнее время — взлом сети KA-SAT в 2022 году. О подобных атаках в 2023 году мы не слышали.

Вердикт: прогноз не сбылся ✗

5. Публикация украденных данных станет новым трендом

В апреле мы писали о KelvinSecurity — испаноговорящей группе взломщиков и хактивистов. Ими движут социально-политические и финансовые интересы, но единой стратегии у группы нет. Их целью могут стать как государственные, так и частные организации в любом уголке мира. Скомпрометированные данные они обычно продают в даркнете, мессенджерах или на собственных платформах, а иногда и раздают их бесплатно.

В мае Ars Technica сообщила о компрометации закрытых ключей BootGuard в результате атаки шифровальщика на компанию Micro-Star International (MSI) в марте этого года (прошивка на компьютерах Intel с включенной функцией BootGuard работает, только если она подписана с помощью специального ключа). Если злоумышленник подпишет собственные вредоносные программы с помощью закрытого ключа, компьютеры MSI будут считать их доверенными.

В августе Insikt Group, подразделение Recorded Future по исследованию угроз, сообщило, что группировка BlueCharlie (также известная под именами TAG-53, Blue Callisto, Callisto (или Calisto), COLDRIVER, Star Blizzard (ранее SEABORGIUM) и TA446) с марта этого года зарегистрировала 94 новых домена. Это указывает на то, что хакеры активно меняют свою инфраструктуру в ответ на публичное раскрытие информации о своей деятельности. Злоумышленники занимаются сбором данных для их дальнейшей публикации или проведения кампаний шпионажа. Их жертвами становятся организации из разных отраслей: органы власти, вузы, оборонные предприятия, политические и неправительственные организации, активисты, журналисты, научно-исследовательские организации и национальные лаборатории.

Вердикт: прогноз сбылся ✓

6. Больше APT-групп заменят Cobalt Strike на аналоги

Мы пристально следим за применением таких инструментов. Злоумышленники нередко используют BruteRatel, но Cobalt Strike остается основным фреймворком для атак.

Вердикт: прогноз не сбылся ✕

7. Для доставки вредоносного кода будут использоваться средства SIGINT

В сентябре исследовательская лаборатория the Citizen Lab опубликовала доклад об известном египетском оппозиционере Ахмеде эль-Тантави. Злоумышленники установили на телефон политика шпионскую программу, используя ранее неизвестную уязвимость нулевого дня.

В августе и сентябре, по данным the Citizen Lab, злоумышленники атаковали эль-Тантави по сети с последующей инъекцией кода, которая не требовала никаких действий с его стороны, даже перехода по ссылке.

Эксперты the Citizen Lab решили найти в сети место внедрения вредоносного кода. Они определили, что источник заражения располагался на стыке сетей двух египетских телеком-провайдеров. Полагаясь на одни технические данные, исследователи не могли точно определить, на чьей стороне находилось промежуточное устройство. Однако они подозревают, что для атаки использовался доступ к базе данных подписчиков одного из провайдеров.

По данными the Citizen Lab, для атаки на эль-Тантави злоумышленникам пришлось бы развернуть систему PacketLogic в телекоммуникационной сети, которой пользуется политик, однако исследователи не обвиняют провайдеров в содействии атакующим в явном виде.

Вердикт: прогноз сбылся ✓

8. Хакеры обратят пристальное внимание на дроны

Несмотря на то что в 2022 году была публикация об атаке дронов на сеть Wi-Fi, в 2023 году информации о подобных инцидентах не появлялось.

Вердикт: прогноз не сбылся ✕

Прогнозы по продвинутым угрозам на 2024 год

1 Больше изобретательных атак на мобильные, носимые и умные устройства

В прошлом году мы столкнулись с новой, необычайно скрытной кампанией кибершпионажа, целью которой были устройства iOS, в том числе принадлежавшие нашим коллегам. Мы назвали ее «Операция Триангуляция». В ходе расследования мы выявили пять уязвимостей в системе iOS, в том числе четыре уязвимости нулевого дня. Они присутствовали и в других ОС и устройствах Apple: не только в смартфонах и планшетах, но и в ноутбуках, носимых гаджетах и устройствах умного дома, в том числе Apple TV и Apple Watch. Полагаем, что в следующем году количество продвинутых атак на гаджеты пользователей и устройства умного дома возрастет. Мишенью не обязательно будут устройства iOS: другие гаджеты и операционные системы могут тоже оказаться под угрозой.

Злоумышленники будут увеличивать масштабы шпионских кампаний, используя уязвимости смарт-камер, систем подключенных автомобилей и так далее. Многие из этих

гаджетов, как новые, так и старые, привлекают злоумышленников своей легкой доступностью — в них полно уязвимостей, ошибок конфигурации и устаревших программ, что делает их идеальной целью для взлома.

Еще одна характерная особенность этой тенденции — «тихая» доставка эксплойта. В «Операции Триангуляция» эксплойты незаметно доставлялись на устройства через сообщения iMessage и активировались без участия пользователя. Не исключено, что в следующем году злоумышленники найдут новые способы доставки эксплойтов, например:

- атаки, не требующие взаимодействия с пользователем, через популярные кросс-платформенные мессенджеры;
- эксплойты одного клика: рассылка в SMS или мессенджерах вредоносных ссылок, переход по которым активирует эксплойт;
- перехват сетевого трафика, например, путем эксплуатации сетей Wi-Fi — этот метод не очень популярен, но довольно эффективен.

Чтобы не стать жертвой сложных и целевых атак, важно защищать как корпоративные, так и личные устройства. Помимо традиционных антивирусных программ, пригодятся XDR-решения и SIEM-платформы, которые обеспечивают централизованный сбор данных, ускоряют анализ и соотносят события безопасности из разных источников, способствуя оперативному реагированию на сложные инциденты.

Мобильные устройства — новая цель для кибератак

Статистика последних лет свидетельствует о значительном росте кибератак, нацеленных на мобильные устройства. По данным аналитиков, в 2019 году количество вредоносных программ и атак на мобильные банковские приложения выросло более чем на 50%. Это делает наши смартфоны и планшеты перспективной целью для хакеров.

На мобильных устройствах мы храним множество личной информации — фотографии, переписку, данные банковских карт. Попадание таких данных в руки злоумышленников чревато серьезными последствиями — от финансовых потерь до кражи личности. Поэтому защита мобильных устройств должна стать приоритетной задачей для каждого.

Вот 5 советов, которые помогут обезопасить ваш смартфон или планшет от кибератак:

- Используйте надежные пароли и двухфакторную аутентификацию. Слабые пароли — наиболее распространенная причина взлома смартфонов.
- Своевременно устанавливайте все обновления ОС и приложений. Они часто содержат важные исправления уязвимостей.
- Ограничьте доступ приложений к личным данным. Многие приложения запрашивают избыточные разрешения.
- Используйте VPN и антивирусные программы для мобильных устройств. Это позволит обезопасить трафик и защитить от вредоносного ПО.
- Не открывайте подозрительные вложения и ссылки в SMS и мессенджерах — это распространенный способ распространения вредоносного кода.

Соблюдение этих простых рекомендаций существенно снизит риски кибератак на ваше мобильное устройство. Будьте бдительны и регулярно проверяйте настройки безопасности!

IoT и 5G: новая эра технологий и вызовы кибербезопасности

Устройства Интернета вещей (IoT) стремительно набирают популярность и в ближайшие годы их число будет только расти. Параллельно развиваются сети 5G, которые открывают новые возможности для IoT за счет высоких скоростей и низких задержек.

Однако вместе с преимуществами этих технологий появляются и новые вызовы для кибербезопасности. Чем больше подключенных устройств, тем выше риски хакерских атак и уязвимостей.

Уже сегодня обнаруживаются серьезные угрозы безопасности в популярных приложениях и ОС, включая Chrome и Android. Архитектура 5G является относительно новой, и требуются дополнительные исследования, чтобы выявить и устранить потенциальные лазейки.

Чтобы свести к минимуму риски, производителям IoT-устройств и разработчикам 5G нужно:

- Внедрять современные стандарты безопасности и шифрования данных
- Проводить тщательное тестирование на проникновение и уязвимости
- Своевременно устанавливать обновления для исправления ошибок
- Использовать аутентификацию и ограничение прав доступа к устройствам
- Обучать пользователей основам кибергигиены

Только комплексный подход позволит минимизировать угрозы и использовать в полной мере потенциал IoT и сетей 5G, не рискуя безопасностью пользователей

Расцвет автомобильного хакинга

Современные автомобили оснащаются автоматизированным программным обеспечением, которое позволяет бесперебойно взаимодействовать с водителями при использовании круиз-контроля, синхронизации работы двигателя, управления замками дверей, активации подушек безопасности и применении передовых систем помощи водителю. Для обеспечения связи в таких автомобилях применяются технологии Bluetooth и Wi-Fi, что также подвергает их риску кибератак со стороны хакеров.

К 2024 году ожидается рост случаев удаленного захвата управления автомобилем и использования микрофонов для подслушивания по мере распространения автоматизированного транспорта. Автономные автомобили используют ещё более сложные механизмы, требующие строгих мер кибербезопасности.

По мере того, как автомобили всё чаще подключаются к интернету, они также становятся более уязвимыми для кибератак. Компаниям следует принимать адекватные меры по обеспечению безопасности подключенных автомобилей, в частности использовать шифрование, аутентификацию и мониторинг в режиме реального времени.

Как защитить автомобиль от взлома

Шифрование данных: Вся информация, передаваемая между автомобилем и другими устройствами, должна быть обязательно зашифрована. Это включает в себя данные, передаваемые через Bluetooth, WiFi и другие средства связи. Использование надежных алгоритмов шифрования поможет защитить информацию от несанкционированного доступа.

- Аутентификация и авторизация: Подключенные устройства должны проходить строгую

процедуру аутентификации перед получением доступа к автомобилю. Это может включать в себя использование надежных паролей или биометрических методов. Кроме того, автомобиль должен иметь четкие правила доступа, чтобы предотвратить несанкционированный доступ к различным функциям.

- Мониторинг в реальном времени: Создание системы мониторинга в реальном времени поможет быстро выявлять необычную активность или атаки. Это позволит оперативно принимать меры по предотвращению угроз, а также поможет обнаруживать уязвимости, которые могут быть использованы злоумышленниками.
- Обновления и патчи безопасности: Производители автомобилей должны регулярно выпускать обновления и патчи безопасности для своего программного обеспечения. Это поможет устранить известные уязвимости и улучшить защиту автомобиля.
- Обучение водителей и владельцев автомобилей: Важно обучать водителей и владельцев автомобилей правилам безопасности. Они должны знать, как обеспечить защиту своих устройств и личных данных при использовании подключенных автомобилей.

Для защиты подключенных автомобилей необходим комплексный подход, включающий шифрование данных, аутентификацию пользователей, мониторинг в реальном времени, регулярное обновление ПО и обучение водителей правилам кибербезопасности. Только такая всесторонняя защита позволит снизить риски кибератак и обеспечить конфиденциальность личных данных владельцев подключенных автомобилей.

2 Новые ботнеты на базе потребительских и корпоративных приложений и устройств

Ни для кого не секрет, что уязвимости есть в любых популярных программах и устройствах, предназначенных как для личного, так и для корпоративного использования. Мы регулярно обнаруживаем новые опасные и критические уязвимости. По данным Statista, в 2022 году было обнаружено рекордное число новых уязвимостей — более 25 тысяч. Компаниям зачастую не хватает ресурсов для работы с уязвимостями и их своевременного исправления. Все это может привести к незаметному созданию новых, масштабных ботнетов, способных проводить целевые атаки.

Для создания ботнета нужно установить вредоносное ПО на множество устройств втайне от их хозяев. Эта тактика может заинтересовать APT-группы по нескольким причинам. Прежде всего, она позволяет злоумышленникам скрыть целенаправленный характер атаки: из-за большого количества атакованных устройств защитникам будет сложно определить автора и мотивы атаки. К тому же ботнеты, созданные на базе устройств, принадлежащих рядовым пользователям или легитимным организациям, служат прекрасной маскировкой для истинной инфраструктуры хакеров. Они могут выполнять роль прокси-серверов или промежуточных командных серверов, а если атака полагается на ошибки в конфигурации сети, они могут стать точкой входа в инфраструктуру организации.

Сами по себе ботнеты — явление не новое. Например, несколько лет назад ботнет, состоящий более чем из 65 000 домашних маршрутизаторов, использовался для перенаправления вредоносного трафика других ботнетов и APT-групп. В другом случае APT-группы атаковали удаленных сотрудников, заражая их маршрутизаторы,

предназначенные для малого и домашнего офиса, троянцами (RAT) и создавали из них своеобразный ботнет. Поскольку в последнее время было обнаружено огромное число уязвимостей, мы считаем, что в следующем году пользователи столкнутся с новыми вариациями таких атак.

Помимо APT-групп, этот метод могут взять на вооружение и киберпреступники. Такие атаки открывают злоумышленникам широкие возможности проникновения в целевую инфраструктуру и закрепления в ней, а их скрытый характер позволяет им оставаться незамеченными.

3 Станет больше успешных атак с выполнением кода на уровне ядра (руткиты режима ядра снова в деле)

С внедрением современных инструментов безопасности в последние релизы Windows, таких как KMCS (подпись кода в режиме ядра), PatchGuard, HVCI (целостность кода, защищенная гипервизором) и архитектура Secure Kernel, корпорация Microsoft планировала сократить количество руткитов и аналогичных низкоуровневых атак. Такие атаки были распространены ранее, во времена относительной популярности руткитов. Однако и сейчас, несмотря на новейшие механизмы защиты, APT-группировкам и другим злоумышленникам удаётся успешно исполнять свой код в режиме ядра на компьютерах жертв. В этом году произошло несколько атак с использованием уязвимости WHCP (программы совместимости оборудования Windows), которые привели к компрометации модели доверенного ядра Windows. В июне 2021 года появились сообщения о рутките Netfilter, после чего корпорация Microsoft опубликовала предупреждение о том, что использовался он для подмены данных о местоположении на китайских игровых платформах. В октябре того же года компания Bitdefender сообщила о рутките FiveSys, который атаковал геймеров во время онлайн-игр. Основной целью злоумышленников являлась кража идентификационных и платежных данных игроков. Позже компания Mandiant обнаружила зловред Poortry, который засветился в нескольких кибератаках, в том числе с использованием шифровальщиков. В июне 2023 года мы опубликовали закрытый отчет о новых подписанных экземплярах FiveSys.

Мы предполагаем, что в следующем году будут развиваться три ключевые тенденции:

- на черном рынке повысится спрос на EV-сертификаты и скомпрометированные сертификаты подписи кода;
- злоумышленники будут чаще взламывать аккаунты разработчиков, чтобы подписывать вредоносный код через службы подписи Microsoft, такие как WHCP;
- все больше злоумышленников будут брать на вооружение технику BYOVD, которая предполагает установку на устройство уязвимого драйвера.

4 Рост числа атак, финансируемых государствами

В прошлом году в мире было более 50 активных международных конфликтов. При этом, по оценкам ООН, мир наблюдал самое большое число вооруженных конфликтов со времен Второй мировой войны. Информационные технологии стали неотъемлемой частью любого конфликта: в наши дни ни одна политическая конфронтация не обходится без кибератак, и мы ожидаем дальнейшего развития этой тенденции. Одним из самых ярких

примеров политического использования зловредов можно считать APT-атаки BlackEnergy на территории Украины в прошлом десятилетии, в которые входили кампании кибершпионажа, деструктивные атаки против медиакомпаний, и компрометация автоматизированных систем управления технологическими процессами. Злоумышленники все чаще используют свой арсенал для поддержки той или иной стороны современных вооруженных конфликтов: например, в зоне российско-украинского конфликта мы выявили APT-кампанию CloudWIzard, а во время конфликта между Израилем и ХАМАС на энергетические, оборонные и телекоммуникационные предприятия Израиля обрушилась целая серия кибератак, за которыми стояла группа хакеров под названием Storm-1133. В это же время многие израильские пользователи устройств Android пострадали от вредоносной версии приложения RedAlert — Rocket Alerts. С другой стороны конфликта группа Predatory Sparrow, по данным CyberScoop, стала снова активна после годового перерыва.

Мы считаем, что по мере нарастания геополитического напряжения возрастет и число финансируемых государствами кибератак. Под прицел попадут не только критически важные элементы инфраструктуры, государственные учреждения и оборонные предприятия по всему миру, но и СМИ. В условиях геополитического кризиса злоумышленники могут попытаться использовать СМИ для пропаганды или дезинформации населения.

Большинство атак будут проводиться с целью кражи данных, повреждения IT-инфраструктуры и длительного шпионажа. Скорее всего, возрастет и количество кибердиверсий. Злоумышленники не станут ограничиваться шифрованием данных: они будут уничтожать их, чтобы причинить серьезный ущерб политическим организациям. Не исключены и целевые атаки против отдельных людей и групп, в том числе компрометация личных устройств для проникновения в организацию, в которой работает жертва, использование дронов для определения местоположение цели, прослушка при помощи вредоносного ПО и так далее.

5 Хактивисты в кибервойне: новая реальность геополитических конфликтов

Хактивизм — еще один пример использования цифровых технологий в зоне конфликтов. Полагаем, что в будущем без хактивистов не обойдется ни одно противостояние. Есть несколько основных направлений их деятельности. Прежде всего, они могут проводить обычные кибератаки, например DDoS-атаки, кражу и уничтожение данных, взлом сайтов и искажение контента и так далее. Кроме того, они могут делать ложные сообщения о взломах, которые повлекут ненужные расследования и приведут к усталости от оповещений среди аналитиков SOC и исследователей кибербезопасности и снижению их бдительности. Так, во время текущего конфликта между Израилем и ХАМАСом группа хактивистов заявила об атаке на частную тепловую электростанцию Дорад в Израиле, которую она якобы совершила в начале октября. Во время расследования оказалось, что опубликованные хактивистами данные были скомпрометированы другой группировкой еще в июне 2022 года. В итоге экспертам пришлось потратить драгоценное время, чтобы выяснить, что никакой новой утечки на самом деле не было. Нередко хактивисты прибегают к дипфейкам — это легкодоступные инструменты для имитации изображения или голоса человека и распространения дезинформации. Бывали и другие громкие случаи, например захват хакерами эфира иранского

государственного телеканала во время протестов. Борьба геополитических сил на мировой арене продолжается, и вряд ли мы дождемся ослабления этого напряжения в ближайшее время. Мы считаем, что на этом фоне возрастет и активность хактивистов, которые будут проводить разрушительные атаки и распространять ложную информацию.

6 Атаки на цепочки поставок как услуга

В последнее время злоумышленники, преследуя свои цели, все чаще начинают атаку с промежуточного звена — поставщиков, интеграторов и разработчиков. Небольшие компании, которым часто не хватает ресурсов для надежной защиты от APT-атак, становятся для них одной из ступенек на пути к конечной цели — данным и инфраструктуре крупных предприятий. Чтобы оценить текущий масштаб атак на цепочки поставок, достаточно вспомнить горячо обсуждаемые взломы Okta в 2022 и 2023 годах. Okta — поставщик услуг аутентификации, обслуживающий более 18 000 клиентов по всему миру, каждый из которых мог стать жертвой злоумышленников.

Атакующие могут действовать из разных побуждений — от жажды наживы до кибершпионажа, что еще раз подчеркивает особую опасность этой угрозы. Например, знаменитая APT-группа Lazarus активно осваивает новые методы атаки на цепочки поставок. Любопытно, например, что известный бэкдор Gopuram, поразивший пользователей по всему миру в результате взлома 3CX, сосуществует в атакованных системах с бэкдором AppleJeus, приписываемым группе Lazarus. Эта высокопрофильная целевая атака была направлена в основном против криптовалютных компаний, и, скорее всего, главной целью злоумышленников было получение финансовой прибыли.

Мы предполагаем, что, учитывая рост популярности атак на цепочки поставок, 2024 год ознаменуется новым этапом их развития. Есть несколько вариантов того, что именно это может быть. Начнем с того, что злоумышленники могут использовать популярное ПО с открытым исходным кодом для атаки на разработчиков, работающих на потенциальную компанию-жертву. Также на теневом рынке могут появиться новые предложения, в том числе наборы доступов к клиентам определенных разработчиков ПО или IT-интеграторов. Доступ к обширной базе потенциальных жертв дает злоумышленникам возможность тщательно отбирать цели для проведения масштабных (и максимально прибыльных) атак. Таким образом, эта активность может выйти на новый уровень.

7 Целевые фишинговые операции на основе генеративного ИИ

Теперь уже никого не удивишь чат-ботами и инструментами для работы с генеративным ИИ — они широко распространены и легко доступны. Злоумышленники тоже не остались в стороне и активно разрабатывают собственные вредоносные чат-боты на базе легитимных решений. WormGPT — одна из таких разработок. Эта языковая модель создана специально для преступных целей на базе GPTJ — языковой модели с открытым исходным кодом. Есть и другие теневые модели, такие как xxxGPT, WolfGPT, FraudGPT, DarkBERT. В них нет функции ограничения контента, как в легитимных решениях, поэтому злоумышленники активно используют их в злонамеренных целях.

Это идеальные инструменты для создания сообщений целевого фишинга — а именно с

них чаще всего начинаются APT- и другие атаки. Но быстрое создание грамотных и убедительных сообщений — это далеко не все. Эти инструменты способны генерировать документы, с помощью которых атакующие смогут выдавать себя за партнеров или коллег своей жертвы, имитируя их стиль. Мы считаем, что в следующем году мы увидим новые методы для автоматизации шпионажа, например автоматизация сбора данных об онлайн-активности пользователя — публикациях в соцсетях, комментариях и собственных статьях. С помощью генеративных инструментов злоумышленники будут обрабатывать такую информацию и на ее основе создавать текстовые и аудиосообщения, имитируя индивидуальный стиль и голос человека.

Вместе с тем будет возрастать необходимость повышения осведомленности о киберугрозах и значимость превентивных мер, таких как анализ угроз, проактивный мониторинг и обнаружение.

Потенциал искусственного интеллекта (ИИ)

С внедрением искусственного интеллекта во все сферы рынка, эта технология в сочетании с машинным обучением привела к колоссальным изменениям в области кибербезопасности. ИИ сыграл ключевую роль в создании автоматизированных систем безопасности, обработке естественного языка, распознавании лиц и автоматическом обнаружении угроз. Однако он также используется для разработки интеллектуальных вредоносных программ и атак, позволяющих обходить передовые протоколы безопасности при контроле данных.

Системы обнаружения угроз на базе искусственного интеллекта способны предсказывать новые кибератаки и мгновенно оповещать администраторов о любых утечках данных. ИИ помогает оперативно обнаруживать и предотвращать кибератаки, а также автоматизировать рутинные задачи. Однако организациям необходимо принимать адекватные меры для защиты от потенциальных угроз, связанных с применением искусственного интеллекта в киберпреступности.

Только комплексный подход к безопасности позволит максимально использовать преимущества ИИ и свести к минимуму риски его злоупотребления.

8 Вырастет число наемных хакеров

Наемные хакеры — это группы, которые предлагают услуги по проникновению в системы жертвы и краже данных. Они работают с частными детективами, юридическими фирмами, бизнес-конкурентами и теми, кому не хватает технических знаний и навыков для проведения подобных атак. Злоумышленники открыто рекламируют свои услуги и атакуют интересующие их цели.

Среди наемных групп, которые отслеживает наш центр глобальных исследований и анализа угроз (GReAT) можно отметить DeathStalker. Главные цели этих злоумышленников — юридические и финансовые организации, но вместо традиционных APT-атак группировка сосредоточилась на услугах взлома и торговле информацией. Злоумышленники рассылают целевые фишинговые письма с вредоносными вложениями, чтобы получить контроль над устройством жертвы и украсть конфиденциальные данные.

Такие группы состоят из профессиональных хакеров, которые объединены в несколько команд, организованных в четкую иерархическую структуру с менеджерами и подчиненными. Они ищут клиентов в теневом интернете, предлагая разные техники взлома — вредоносное ПО, фишинг и другие методы социальной инженерии, и т. д. Они действуют анонимно и используют VPN, чтобы избежать обнаружения, а их действия приводят к самым разным последствиям — от утечки данных до репутационного ущерба. Как правило, в услуги наемных хакеров входит не только кибербразведка, но и коммерческий шпионаж. В их руках могут оказаться практически любые данные об участниках рынка, например сведения о реорганизации, планы расширения деятельности, финансовая информация и данные о клиентах.

Такие услуги пользуются большим спросом по всему миру, и мы ожидаем их дальнейшей популяризации в следующем году. Возможно, в ответ на запросы теневого рынка некоторые APT-группы расширят спектр операций, чтобы поддерживать свою деятельность, оплачивать услуги агентов и получать прибыль.

9 Новые атаки через MFT-системы

По мере развития цифровых технологий растет и сложность киберугроз. Новый сценарий кибератак будет развиваться вокруг MFT-систем (Managed File Transfer, управляемый обмен файлами), которые предназначены для безопасного обмена конфиденциальными данными между организациями. MFT-системы хранят огромные объемы конфиденциальной информации, в том числе финансовую отчетность, данные клиентов и сведения, составляющие коммерческую тайну, и давно стали неотъемлемой частью современных бизнес-процессов. Они упрощают передачу данных внутри организации и обмен данными с другими компаниями, повышая эффективность бизнес-операций. Но в связи с тем, что эти системы играют такую важную роль в работе организаций, они стали привлекательной целью для злоумышленников, жаждущих заработать на цифровых уязвимостях.

В 2023 году мы наблюдали несколько атак на MFT, в частности MOVEit и GoAnywhere, которые пролили свет на потенциальные уязвимости этих важнейших систем передачи данных. Взлом MOVEit, за которым стоит группа вымогателей Cl0p, и эксплуатация уязвимости MFT-платформы GoAnywhere, разработанной компанией Fortra, еще раз показали, как одна-единственная уязвимость может привести к эксфильтрации конфиденциальных данных, остановке бизнес-процессов и шантажу.

Мы считаем, что впереди нас ждет еще немало целевых атак на MFT-системы: они способны не только принести злоумышленникам финансовую выгоду, но и остановить бизнес-процессы в атакованной компании. Сложная архитектура MFT-систем, интегрированная в обширные корпоративные сети, может иметь много уязвимостей, которыми с готовностью воспользуются атакующие. Злоумышленники неустанно совершенствуют свои навыки и, скорее всего, будут активнее эксплуатировать уязвимости MFT-систем в ближайшем будущем.

Судя по наметившейся тенденции, взломов MFT с серьезными утечками данных и вымогательством в ближайшем будущем будет больше. Инциденты, которые мы наблюдали в 2023 году, настойчиво напоминают о том, что MFT-системы не лишены уязвимостей и

требуют надежной защиты от кибератак, нацеленных на кражу данных.

Именно поэтому организациям настоятельно рекомендуется тщательно проверять используемые MFT-системы, чтобы вовремя выявлять и устранять потенциальные уязвимости. Надежные технологии предотвращения утечек данных (DLP), шифрование конфиденциальной информации и повышение осведомленности сотрудников о кибербезопасности помогут защитить MFT-системы от новейших угроз. Для защиты корпоративных данных и обеспечения непрерывности бизнес-процессов на фоне растущего ландшафта киберугроз компаниям следует принимать проактивные меры, в том числе по повышению безопасности MFT-систем.

События 2023 года еще раз напомнили компаниям о необходимости укрепления защиты MFT-систем. В будущем кибератаки станут еще запутанней, поэтому каждой организации крайне важно всегда оставаться на шаг впереди злоумышленников и поддерживать целостность и безопасность MFT-систем, чтобы не пополнить список пострадавших компаний.

Облачные хранилища: как обезопасить данные

В настоящее время все больше компаний переходят на работу с данными в облаке. Это позволяет повысить мобильность сотрудников и снизить издержки на ИТ-инфраструктуру. Однако вместе с преимуществами облачных сервисов растут и риски кибербезопасности.

Крупные облачные провайдеры, такие как Google, Microsoft и Amazon, отличаются высоким уровнем защиты данных со своей стороны. Однако основные угрозы исходят со стороны пользователей. Распространенными проблемами являются:

- Ненадежные пароли доступа к облаку
- Загрузка зараженных файлов
- Некорректная настройка прав доступа
- Устаревшее ПО и отсутствие своевременных обновлений
- Фишинговые атаки и вредоносные программы

Чтобы минимизировать риски и обеспечить безопасность данных в облаке, эксперты рекомендуют:

- Использовать многофакторную аутентификацию
- Применять средства защиты от вредоносного ПО
- Регулярно обновлять ПО и настройки безопасности
- Ограничивать доступ и использовать шифрование
- Проводить аудит активности и своевременно устранять уязвимости
- Регулярно делать резервное копирование данных

Следование этим простым правилам позволит максимально обезопасить ценные данные вашей компании в облачных хранилищах от кибератак и утече

Нарушение целостности данных: Главная мишень кибератак

В эпоху цифровизации данные становятся одним из важнейших активов как для компаний, так и для частных пользователей. Однако вместе с этим растут и угрозы безопасности персональных данных.

Любые уязвимости в системах и приложениях открывают потенциальные возможности для хакерских атак и утечек конфиденциальной информации. По статистике, две трети всех утечек данных происходят из-за ошибок пользователей, устаревшего ПО или некорректных настроек безопасности.

Чтобы свести к минимуму риск компрометации данных, компании и частные пользователи должны:

- Регулярно обновлять ПО, в том числе антивирусные базы
- Внедрять решения для защиты от утечек данных
- Шифровать конфиденциальную информацию
- Ограничивать и регулировать права доступа сотрудников к данным
- Соблюдать требования регуляторов по защите персональных данных

В частности, в ЕС с 2018 года действует жесткий регламент GDPR, а в Калифорнии — закон CCPA о защите прав потребителей. Их несоблюдение грозит крупными штрафами.

Таким образом, обеспечение целостности и конфиденциальности данных должно стать приоритетной задачей кибербезопасности для любой компании. Только комплексный подход позволит минимизировать риски хакерских атак и утечек.

Целевые программы — вымогатели — растущая опасность ransomware (программа-вымогатель)

В последние годы все большее распространение получают целевые программы-вымогатели. В отличие от массовых атак, они нацелены на конкретные организации и отрасли.

Особенно уязвимы компании, сильно зависящие от специализированного ПО в повседневной деятельности. Например, атака WannaCry при помощи вредоносного ПО-вымогателя поразила более 70 тысяч медицинских устройств в больницах Великобритании.

Ключевые особенности целевого ransomware:

- Направлен на конкретную жертву, а не массовое заражение
- Использует векторы атаки, характерные для цели
- Шифрует важные для бизнеса данные
- Запрашивает крупный выкуп за расшифровку

Чтобы снизить риски подобных атак, эксперты рекомендуют:

- Регулярно обновлять и тестировать системы безопасности
- Делать резервные копии и архивы данных
- Обучать персонал основам кибергигиены
- Использовать надежные решения для защиты от вредоносного ПО

Целевой ransomware способен нанести огромный ущерб ключевым системам и бизнес-процессам. Поэтому защита от таких угроз должна стать приоритетом для любой компании.

Инсайдерские угрозы — ахиллесова пята кибербезопасности

Человеческий фактор остается одной из главных проблем кибербезопасности. Согласно

отчету Verizon, 34% всех утечек данных так или иначе связаны с действиями сотрудников компаний.

Причины инсайдерских угроз:

- Небрежность и ошибки персонала при работе с данными
- Намеренные злонамеренные действия (кража данных, мошенничество и др.)
- Недостаточная осведомленность сотрудников о правилах кибергигиены
- Устаревшие или избыточные права доступа к системам и данным
- Недовольство компанией, желание отомстить

Чтобы снизить инсайдерские риски, компаниям рекомендуется:

- Проводить регулярное обучение персонала правилам безопасности
- Внедрять системы контроля и анализа действий сотрудников
- Ограничивать и регулировать права доступа к критическим данным
- Своевременно блокировать уволенных сотрудников во всех системах
- Создавать культуру доверия и лояльности в коллективе

Такой комплексный подход поможет минимизировать угрозы изнутри и обезопасить компанию от утечек по вине собственных сотрудников.

Обеспечение кибербезопасности в условиях удаленной занятости

Переход на удаленную работу в период пандемии создал новые вызовы для киберзащиты компаний. Вот основные аспекты, требующие внимания:

- Использование сотрудниками личных незащищенных устройств и сетей, уязвимых для взлома.
- Рост атак методами социальной инженерии — фишинга, вишинга, подбора паролей. Злоумышленники активно используют тему COVID.
- Сложности контроля доступа и поведения персонала при удаленной работе. Риски инсайдерских угроз возрастают.
- Трудности быстрого обнаружения и реагирования на инциденты кибербезопасности.

Для минимизации рисков компаниям рекомендуется:

- Внедрить системы удаленного управления доступом, шифрования и мониторинга.
- Использовать VPN и средства многофакторной аутентификации.
- Проводить регулярное обучение сотрудников кибергигиене.
- Своевременно устанавливать все обновления безопасности.
- Организовать проактивный мониторинг угроз и оперативное реагирование.

Только комплексный подход обеспечит надежную защиту бизнеса в новых условиях.

Автоматизация — ключ к эффективной киберзащите

В условиях стремительного роста объемов данных их защита становится все сложнее. Чтобы обеспечить надежный контроль за информацией, крайне важно внедрять автоматизацию процессов кибербезопасности.

Автоматизация позволяет значительно повысить скорость и эффективность реагирования на инциденты. Это особенно актуально для современных высоконагруженных ИТ-специалистов и инженеров.

Ключевые преимущества автоматизации в кибербезопасности:

- Быстрое обнаружение и реагирование на атаки в режиме реального времени
- Сокращение числа ошибок, связанных с человеческим фактором
- Возможность масштабирования защиты под растущие потребности
- Оптимизация затрат на кибербезопасность за счет сокращения ручного труда
- Улучшение соответствия регуляторным нормам и стандартам

Чтобы извлечь максимум преимуществ, автоматизацию стоит интегрировать в процессы разработки ПО на ранних стадиях. Это позволит создавать более безопасные приложения.

Внедрение автоматизированных решений является важнейшим трендом современной киберзащиты. Это поможет компаниям эффективно противостоять растущим киберугрозам.

Многофакторная аутентификация: надежный щит для бизнеса

В эпоху цифровизации все актуальнее для компаний становится вопрос кибербезопасности. Одним из ключевых инструментов защиты в настоящее время является многофакторная аутентификация (МФА).

МФА подразумевает несколько уровней проверки личности пользователя при входе в систему. Это могут быть пароль, одноразовый код по SMS, сканирование отпечатка пальца или другие методы.

Применение МФА резко снижает риски взлома, поскольку злоумышленнику нужно получить доступ сразу к нескольким элементам аутентификации. По данным аналитиков, МФА сокращает вероятность взлома аккаунтов в 5-10 раз!

Для надежной защиты бизнеса эксперты рекомендуют внедрить МФА для всех сотрудников, особенно имеющих доступ к важным данным и системам. Несмотря на определенные издержки, это многократно окупится за счет предотвращения кибератак, которые могут обойтись компании в миллионы рублей.

МФА — это один из ключевых трендов в сфере кибербезопасности. Внедрение многофакторной аутентификации позволит надежно защитить ценные данные и системы компании от хакерских атак и несанкционированного доступа. Это важнейший инструмент защиты бизнеса в современном цифровом мире.

Управление идентификацией и доступом — ключ к защите данных

В условиях цифровой трансформации бизнеса все большую актуальность приобретает вопрос управления идентификацией и доступом пользователей к корпоративным данным и системам.

Управление идентификацией и доступом (Identity and Access Management, IAM) подразумевает комплекс мер для контроля за тем, кто и на каких условиях может получить доступ к информационным ресурсам компании.

Внедрение надежной системы IAM включает:

- Аутентификацию пользователей на основе паролей, биометрии, многофакторной идентификации
- Установление четких ролей и правил доступа разных категорий сотрудников

- Мониторинг и аудит действий пользователей в системе
- Оперативную блокировку в случае компрометации учетной записи
- Шифрование и анонимизацию данных

Внедрение системы IAM позволяет оптимально защитить критически важные данные компании от утечек и несанкционированного использования. Это ключевой элемент комплексной стратегии кибербезопасности современного бизнеса.

Мониторинг данных в реальном времени: 5 ключевых шагов для обеспечения безопасности данных

Мониторинг данных в реальном времени является критически важным аспектом обеспечения безопасности в мире цифровых технологий. Он позволяет организациям оперативно обнаруживать и реагировать на любые подозрительные действия, что может помочь предотвратить серьезные инциденты. Вот пять ключевых шагов, которые следует учесть при реализации мониторинга данных в реальном времени:

- Определение ключевых инцидентов: Прежде всего, определите, какие события и инциденты следует считать критическими для вашей организации. Это могут быть попытки несанкционированного доступа, аномальная активность пользователей, атаки на системы и другие аспекты, которые могут повлиять на безопасность данных.
- Инструменты мониторинга: Выберите и настройте инструменты мониторинга данных, которые соответствуют вашим потребностям. Эти инструменты могут включать в себя системы журналирования, средства обнаружения аномалий и системы анализа данных в реальном времени.
- Установка правил и порогов: Создайте набор правил и порогов, которые помогут системе мониторинга идентифицировать подозрительные события. Эти правила могут быть связаны с обнаружением необычной активности, атаками или нарушениями политик безопасности.
- Автоматические оповещения: Настройте систему для отправки автоматических оповещений в случае обнаружения подозрительных событий. Это позволит вашей команде быстро реагировать и предпринимать меры по предотвращению угроз.
- Анализ и реагирование: Важно не только обнаруживать инциденты, но и иметь процессы и команду для анализа и реагирования. Разработайте план действий для различных сценариев и убедитесь, что ваша команда знает, как правильно реагировать на угрозы безопасности данных.

Понимание и активная реализация мониторинга данных в реальном времени поможет вашей организации значительно повысить уровень безопасности и защитить ценные данные от угроз.

Тенденции в области кибербезопасности: важность обучения

С учетом вышеизложенных тенденций в области кибербезопасности на 2024 год, организации сталкиваются с необходимостью усилить меры безопасности и вложить дополнительные ресурсы в защиту своих ценных активов. Прогнозируется, что организациями будут направлены более 100 миллиардов долларов на обеспечение безопасности своих данных и инфраструктуры.

Безопасность данных и инфраструктуры становится неотъемлемой частью практически любой организации, стоит задуматься о начале обучения кибербезопасности уже сейчас, чтобы в будущем стать экспертами в этой области. Квалифицированные и опытные специалисты по кибербезопасности входят в число наиболее высокооплачиваемых профессионалов в сфере информационных технологий.

Инвестиции в развитие собственных навыков в области кибербезопасности могут оказаться не только полезными, но и выгодными в долгосрочной перспективе.