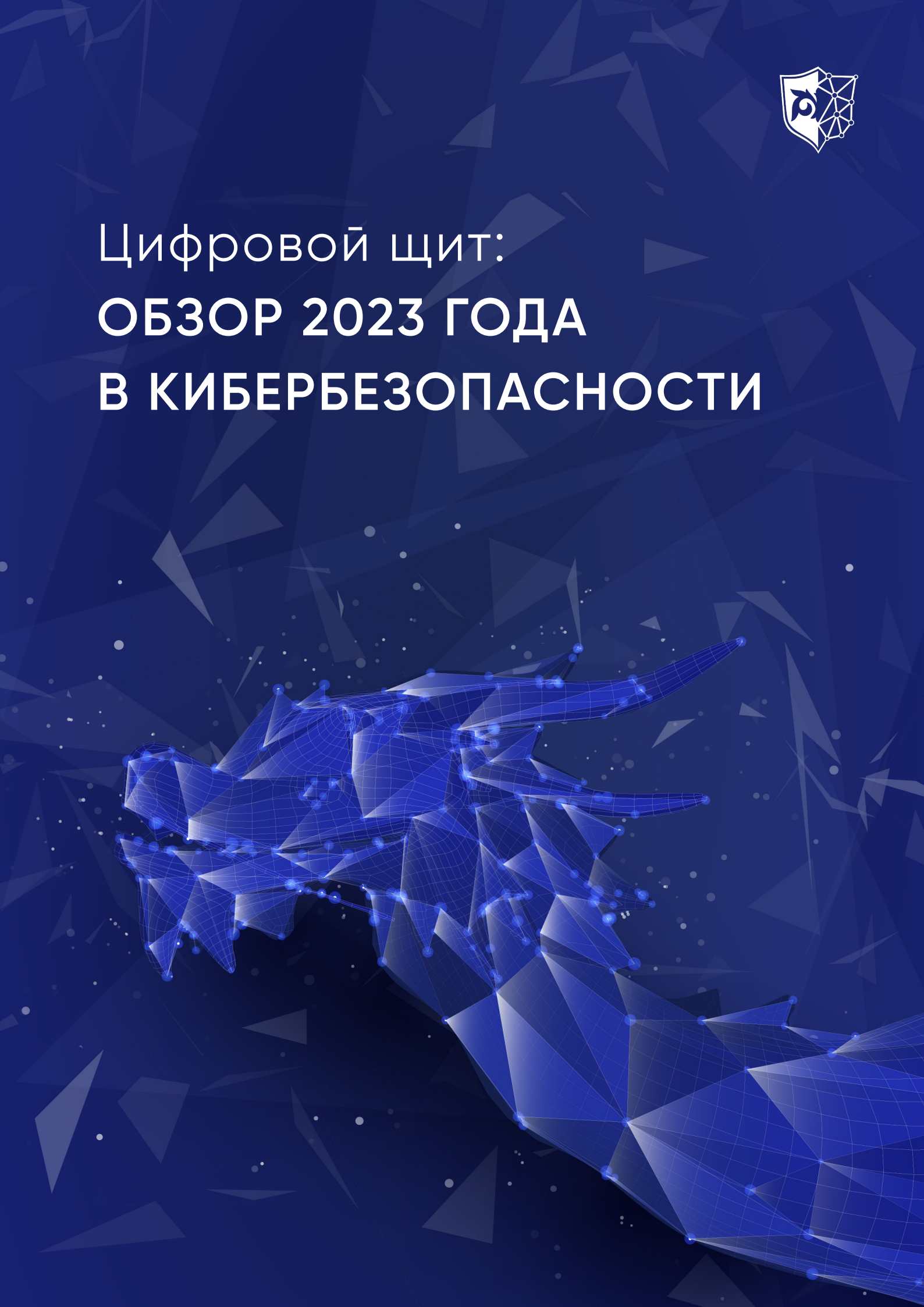
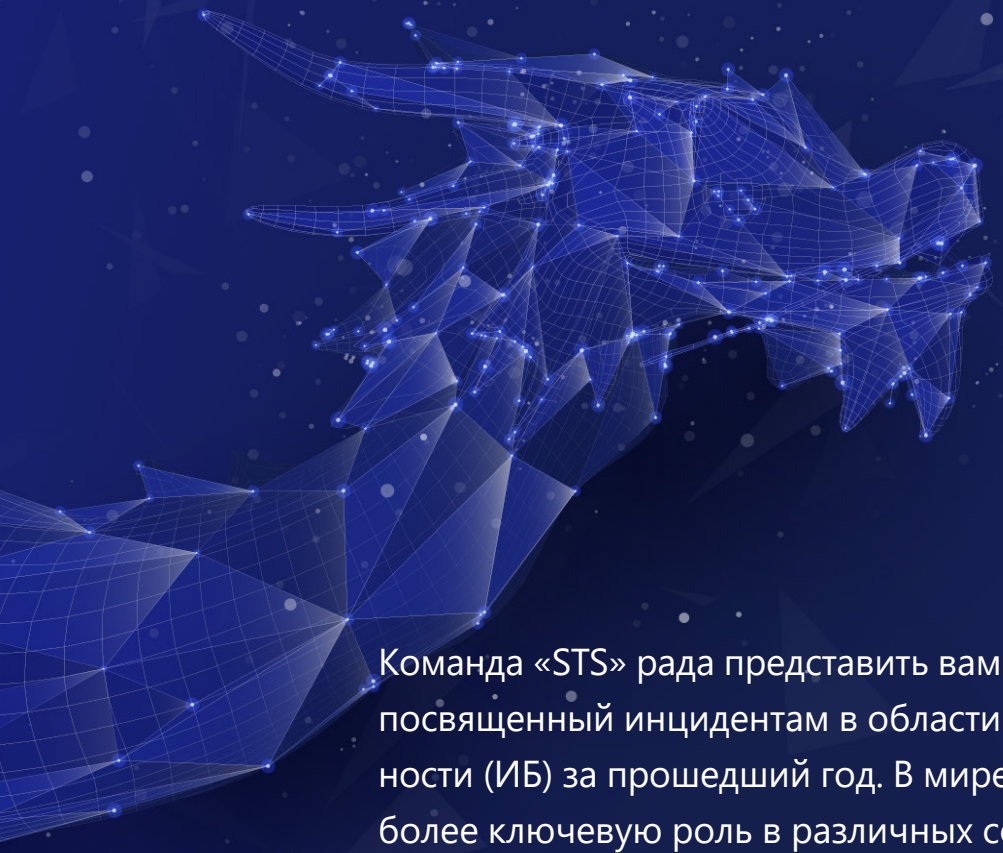
Цифровой щит:
ОБЗОР 2023 ГОДА В КИБЕРБЕЗОПАСНОСТИ



Кибердайджест: Содержание



Дорогие читатели,

Команда «STS» рада представить вам ежегодный кибердайджест, посвященный инцидентам в области информационной безопасности (ИБ) за прошедший год. В мире, где технологии играют все более ключевую роль в различных сферах нашей жизни, вопросы информационной безопасности становятся неотъемлемой частью нашего повседневного существования.

Прошедший год оказался богатым на события и вызовы в области ИБ, с которыми сталкиваются как индивиды, так и организации. Угрозы ИБ постоянно эволюционируют, а киберпреступники находят новые способы атак, чтобы получить доступ к чувствительной информации.

В этом дайджесте мы рассмотрим наиболее значимые и влиятельные инциденты в области ИБ, произошедшие в Казахстане и мире. Мы предоставим анализ тенденций, выявим уроки, которые можно извлечь из произошедших событий, и обсудим стратегии укрепления ИБ нашего общества в будущем.

Следите за нашими аккаунтами в социальных сетях, чтобы быть в курсе последних событий в мире кибербезопасности и понимать, какие шаги нужно предпринять, чтобы защитить себя от возрастающих угроз ИБ.

Будьте в безопасности!

Безопасность в цифровом пространстве становится важнейшим вопросом, требующим постоянного внимания и анализа. С ростом числа цифровых технологий также возрастает и уровень угроз информационной безопасности, с которыми сталкиваются организации и частные лица.

В данном блоке кибердайджеста мы предоставляем краткий обзор последних событий в области информационной безопасности. Погрузимся в мир киберпространства и рассмотрим ключевые инциденты, определяющие текущую картину информационной безопасности в Казахстане.

1 Данные более 260 тысяч казахстанских клиентов магазина «Спортмастер» утекли в сеть

В начале текущего года стало известно об утечке персональных данных клиентов сети спортивных магазинов «Спортмастер» из стран СНГ.

Список содержал в себе более 260 000 строк с данными граждан Казахстана. Актуальность данных охватывает период с 15.09.2012 по 18.05.2018 года.

Файл содержит в себе имена, даты рождения, номера телефонов и адреса электронных почт. Компания «Спортмастер» подтвердила утечку, отметив, что инцидент не затрагивает логины и пароли пользователей, платежную информацию, а также учетные данные сотрудников. Начато внутреннее расследование. По предварительной версии, утечка могла произойти со стороны одного из подрядчиков, имевшего доступ к этой информации. Информацию, полученную в результате утечки, злоумышленники могут использовать в социальной инженерии, а именно при осуществлении звонков и рассылке фишинговых сообщений с целью получения конфиденциальных и банковских данных.

Кроме того, эту же информацию злоумышленники могут использовать при взломе страниц пользователей в социальных сетях, не подключивших двухфакторную аутентификацию.

2 Хакеры требовали биткойны от государственного ведомства РК

В одной из организаций квазигосударственного сектора РК обнаружено заражение сети вирусом-шифровальщиком.

Для дешифровки злоумышленники потребовали выплату в биткойнах.
Предварительный анализ показал, что организация не соблюдала требований

постановления Правительства РК от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

Из всей сети организации злоумышленнику беспрепятственно удалось заразить контроллер домена, три персональных компьютера и файловый сервер. Специалисты установили, что один из персональных компьютеров был зашифрован полностью, а системные логи очищены.

Для всех пользователей организации была создана лишь одна учетная запись — «X». С помощью перебора паролей, используя протокол RDP (протокол удаленного рабочего стола от Microsoft), злоумышленник получил доступ к инфраструктуре и удалил антивирусное программное обеспечение на каждой рабочей станции.

После удаления антивирусного ПО на все устройства был загружен шифровальщик. Зашифрованные файлы получили расширение (CW-WL3048625917) и выполнили команды, предназначенные для остановки различных служб и отключения определенных функций в операционной системе Windows, таких как SQL Server, служба виртуальных дисков, служба теневого копирования томов и брандмауэр Windows.

В придачу шифровальщик скопировал самого себя в папку для установки в автозагрузки, а в каталогах создал файл unlock-info.txt - текст с требованием выкупа.

3 Уязвимость одного образовательного сайта - причина компрометации 40 казахстанских сайтов.

В марте 2023 года обнаружен веб-шелл на одном из интернет-ресурсов частных образовательных учреждений.

Веб-шелл (web-shell) - вредоносный скрипт, который представляет собой серьёзную угрозу безопасности, используется злоумышленниками для управления интернет-ресурсами или веб-серверами.

Для размещения скрипта чаще всего используются уязвимости в коде сайта или подбор паролей. Загрузка веб-шелла осуществляется из-за уязвимостей веб-приложения или неправильной конфигурации. В ходе анализа инцидента информационной безопасности выявлено более 40 интернет-ресурсов, которые находились на данном веб-сервере и, вероятно, уже были скомпрометированы.

Отметим, что данный веб-шелл поддерживает 22 различных набора символов и шифрует исходный код с помощью ключа (пароля) при загрузке, но не содержит этот ключ в полученном файле. Кроме того, веб-шелл имеет скрытый режим и позволяет работать с различными задачами без перезагрузки страницы и потери данных.

Зачастую веб-шеллы трудно обнаружить по причине несложной модификации. Антивирусные продукты иногда не справляются с их обнаружением. Необходимо обратить внимание, что некоторые из этих индикаторов

являются общими для легитимных файлов. Подозрительные вредоносные файлы следует рассматривать в контексте других индикаторов и сортировать, чтобы определить, требуется ли дальнейшая проверка.

На активность веб-шелла также может указывать признак, когда злоумышленник часто посещает только тот URL, где создан сценарий веб-шелла. Обычный пользователь загружает веб-страницу со связанной страницы или загружает дополнительный контент или ресурсы.

Таким образом, частотный анализ журналов веб-доступа может указывать на местонахождение веб-шелла. Большинство легитимных обращений будут содержать различные пользовательские агенты, тогда как веб-шелл может посещаться только злоумышленником, что приводит к ограниченным вариантам пользовательских агентов.

4 Компании, использующие GeoServer, находятся в опасности

В мае 2023 года обнаружено 17 IP-адресов, предположительно подверженных критическим уязвимостям с идентификаторами CVE-2022-24816 и CVE-2023-25157.

Обнаруженные IP-адреса принадлежат крупным компаниям квазигосударственного сектора Казахстана.

GeoServer применяется в различных отраслях, таких как геология, экология, геодезия, сельское хозяйство, управление городами и др., где пространственные данные являются важными компонентами для принятия стратегических решений.

Своевременно непринятые меры по устранению уязвимостей могут привести к компрометации конфиденциальных данных и осуществлению дальнейших атак на сеть, в том числе внедрению вредоносного программного обеспечения в другие системы, что поставит под угрозу безопасность инфраструктуры всей сети.

Успешная атака на уязвимый GeoServer может нанести ущерб репутации компании и привести к негативному вниманию со стороны СМИ и общественности.

«Этот случай еще раз доказывает, что сотрудники отделов информационной безопасности этих отраслей не уделяют должного внимания обновлению компонентов системы, что приводит к удваиванию угроз утечки конфиденциальной информации».

Ранее компания Shadowserver Foundation* опубликовала информацию об уязвимостях в программном обеспечении GeoServer.

** Shadowserver Foundation*
- организация по обеспечению информационной безопасности, которая отправляет ежедневные сетевые отчеты подписчикам и сотрудничает с правоохранительными органами по всему миру в расследовании киберпреступлений.

5 Свыше 17 тысяч роутеров в Казахстане потенциально подвержены уязвимости Mikrotik Routeros

В июле 2023 года в Казахстане выявлено 17 тысяч роутеров, которые потенциально подвержены уязвимости MikroTik. 5 128 роутеров имеют явные признаки ее наличия.

Используя эту уязвимость в своих целях, злоумышленник сможет повысить привилегии с уровня простого администратора до super admin (встроенная учетная запись администратора).

Для эксплуатации уязвимости требуется аутентификация, но даже это не проблема для хакера, ведь в RouterOS по умолчанию установлены стандартные учетные данные администратора. В инструкциях MikroTik по безопасности при установке роутера рекомендовано удалить данные администратора. Проще говоря, заменить пароль, но большинство этих рекомендаций игнорируются.

Организациям, использующим уязвимые версии продукта MikroTik RouterOS, рекомендуется незамедлительно применить обновления из официального источника в соответствии с правилами политики организации.

Отмечается также, что в ранних сборках RouterOS ниже 6.49 заданный по умолчанию админ-пароль представляет собой пустую строку и почти 60% роутеров MikroTik все еще его используют.

6 Инцидент с фальшивым обновлением NCALayer

Известно, что для подписания запроса на получение госуслуги необходимо установить NCALayer.

В сентябре текущего года выявлен фишинговый интернет-ресур ncalayer.info/update.php, при открытии которого под видом обновления для NCALayer загружается и запускается вредоносная программа типа «Trojan Downloader».

После цепочки расшифрования и загрузок, которая включает популярный репозиторий кода GitHub, на компьютер устанавливается вредоносное программное обеспечение Venom RAT v6.0.1, взломанная версия которой распространяется на хакерских даркнет форумах.

Особенностью этой вредоносной программы является то, что она обладает функционалом кейлоггера, кражи данных, скрытного дистанционного управления компьютером (VNC), а также управления веб-камерой.

В конечном результате злоумышленник имеет возможность считывать информацию, набираемую на клавиатуре, просматривать пароли, в т. ч. с браузеров, а также установить сторонние приложения.

7 Хакеры могут взломать казахстанские компании, использующие продукты Citrix

В казахстанском сегменте Интернета в октябре текущего года обнаружены 27 IP-адресов, использующих продукты Citrix NetScaler ADC и NetScaler Gateway, которые потенциально подвержены уязвимости с высоким уровнем критичности идентификатора CVE-2023-3519.

В соответствии с CVSSv3.1 (Common Vulnerability Scoring System) уязвимость имеет рейтинг 9.8 из 10. Она позволяет злоумышленнику выполнять произвольный код без авторизации.

Уязвимость возникает при отправке слишком большого количества методов каноникализации или преобразования в сообщении SAML.

Известно, что в ходе массовых атак на CVE-2023-3519 с 20 июля текущего года около 640 серверов в мире Citrix Netscaler ADC и Gateway уже взломаны и заражены бэкдорами. Также годами ранее вымогательские группировки REvil и DoppelPaymer воспользовались аналогичными уязвимостями Citrix Netscaler ADC и Gateway для взлома корпоративных сетей в прошлых атаках.

Необходимо отметить, что злоумышленник, воспользовавшись уязвимостью, может внедрить вредоносное ПО, похитить конфиденциальные данные и произвести дальнейшие атаки на сеть, что поставит под угрозу безопасность инфраструктуры всей сети.

8 Причина утечки персональных данных казахстанцев – инфостилер

В ноябре 2023 года зафиксировано увеличение количества инцидентов информационной безопасности, связанных с утечкой персональных данных.

Причиной утечки являются инфостилеры, вредоносные программные обеспечения *(далее – ВПО)*, которые нацелены на кражу личных данных *(пароли, банковские данные и другие чувствительные сведения)* с зараженных компьютеров. Этот тип ВПО создан для скрытой работы и передачи украденных данных злоумышленникам.

Инфостилеры *(или информационные трояны)* - это вид ВПО, разработанных для сбора конфиденциальных данных с ПК жертвы. Они крадут личные данные, такие как учетные записи, пароли, номера кредитных карт и другие конфиденциальные сведения.

Существует подвид инфостилеров – кейлоггеры, которые регистрируют нажатия клавиш пользователя. Они тоже предназначены для сбора конфиденциальной информации пользователя.

Некоторые инфостилеры, которые были причиной утечки персональных данных:

ReadLine Stealer

Продается на закрытых форумах и используется злоумышленниками для кражи данных и загрузки других вирусов на устройство жертвы.
Может воровать логины, пароли, данные автозаполнения, файлы cookie и данные кредитных карт из всех веб-браузеров. Хакеры могут неправомерно использовать эту информацию для доступа к различным учетным записям *(например, к социальным сетям, электронной почте, банковским счетам, криптовалютным кошелькам)*.

Vidar Stealer

Это инфостилер, который способен похищать и передавать на сервер злоумышленника чувствительные данные с компьютера жертвы, включая банковскую информацию, сохраненные пароли, IP-адреса, историю браузера, учетные данные для входа в криптокошельки. Vidar Stealer распространяется с помощью спам-писем, пиратского ПО, генераторов ключей и т.д.

Raccoon Stealer

Предназначен для кражи данных с ПК и систем. Это типичный представитель категории инфостилеров, которые направлены на сбор конфиденциальной информации, такой как логины и пароли от учетных записей, данные банковских карт и другие личные сведения. Распространяется различными способами, включая вредоносные вложения в электронной почте, компрометированные веб-сайты, или через эксплойты в ПО. Как правило, их целью является незаметное проникновение на целевые системы, чтобы собирать информацию, не привлекая внимание.

Azorult Stealer

Часто используется для сбора данных, таких как логины, пароли, данные банковских карт, информация о cookie браузера и других ценных сведений. Может распространяться через вредоносные электронные письма, вредоносные веб-сайты, компрометированные программы или эксплойты. После заражения собирает информацию, которую затем отправляет на удаленный сервер, контролируемый злоумышленниками.

Когда речь идет об утечке персональных данных из-за инфостилера, это чаще значит, что произошло крупное нарушение информационной безопасности.

Обычно такие ситуации требуют серьезного расследования и принятия мер для предотвращения подобных инцидентов в будущем.

В связи со стремительными темпами развития технологий в мире обеспечение информационной безопасности становится непрерывным вызовом.

Обзор последних инцидентов в области информационной безопасности в Казахстане подчеркивает важность постоянного мониторинга и адаптации к новым угрозам цифровой среды. Фишинговые атаки, вредоносные программы и другие киберугрозы становятся все более сложными и изощренными.

Стоит отметить, что информационная безопасность - это непрерывный процесс, требующий внимания и обновления стратегий. Постоянное обучение, инновационные подходы и совместные исследования обеспечат необходимый уровень защиты в цифровой эпохе.

Кибергигиена.

Повышение осведомленности среди пользователей

Осведомленность об информационной безопасности является ключевым аспектом нашего стремления к созданию безопасного цифрового пространства для сотрудников казахстанских организаций, обычных пользователей и общества в целом.

Команда «STS» реализует **разнообразные мероприятия по повышению уровня культуры информационной безопасности (ИБ), охватывая различные аудитории, включая сотрудников организаций различных секторов, казахстанских пользователей, в том числе школьников и студентов.**

Команда «STS» регулярно проводит лекции на разнообразные темы по кибергигиене, включая основные аспекты безопасного использования интернета, защиты от фишинга, обзор современных угроз ИБ, и т.д. Лекционные мероприятия направлены на повышение общей осведомленности и обучение практическим навыкам безопасности пользователей в цифровом мире.

В настоящее время растет процентная доля целевых фишинговых атак, организуемых через рассылку писем по электронной почте в адрес сотрудников государственных органов Республики Казахстан, квазигосударственного и частного секторов.

Сотрудники получают **тщательно разработанные** фишинговые[1] сообщения, провоцирующие сотрудника вводить **конфиденциальные/персональные сведения –логин и пароль,** которые дают доступ к корпоративным сетям или базам данных с конфиденциальной или персональной информацией Организации.

Целевые[2] фишинговые письма могут содержать ВПО, в большинстве случаев это программное обеспечение для удаленного доступа, вредоносного загрузчика или вируса-шифровальщика.

Технические меры защиты от Фишинга, такие как **фильтрация и анализ почтового/веб-трафика, ограничение программной среды, запрет запуска вложений/ПО** - весьма эффективны, но при этом они не могут **противостоять новым угрозам и, что более важно, не могут противостоять человеческой любознательности и неосведомлённости.** В этой связи одним из важных факторов защиты от целевых фишинговых атак является **обучение сотрудников.**

[1] «Фишинг» (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

[2] «Спирфишинг» (англ. spear phishing) – вид Фишинга, при котором злоумышленник формирует фишинговое письмо под конкретного получателя, используя собранные ранее данные о получателе.

Проведение киберучений (практических тестов на фишинг и другие виды атак) среди сотрудников организации играет важную роль в повышении культуры информационной безопасности и осведомленности пользователей по реагированию на угрозы и инциденты информационной безопасности по следующим причинам:

Идентификация слабых мест

Киберучения помогают выявить уязвимые места в системе обеспечения информационной безопасности.
Если сотрудники уязвимы для фишинга или других атак, это может стать точкой входа для злоумышленников. Проведение таких тестов позволяет организации увидеть, где нужно улучшить защиту.

Обучение и осведомленность

Киберучения не только идентифицируют проблемы, но и обучают сотрудников распознавать и реагировать на потенциальные угрозы.
Это помогает повысить уровень информационной грамотности и осведомленности сотрудников, делая их более готовыми к действиям в случае инцидентов.

Формирование лучших практик

Через проведение киберучений организация может разрабатывать и распространять наилучшие практики в области информационной безопасности среди своих сотрудников. Это может включать в себя правила по проверке электронной почты, ссылок и вложений, а также инструкции по созданию и управлению паролями.

Тестирование стратегий реагирования

Проведение киберучений позволяет проверить эффективность планов и стратегий реагирования на инциденты информационной безопасности. Если сотрудники успешно распознают и реагируют на атаку в рамках учения, это дает уверенность в том, что планы и стратегии готовы к применению в реальных ситуациях.

Уменьшение рисков

Повышение информационной безопасности означает уменьшение риска инцидентов, которые могли бы привести к утечке конфиденциальной информации, финансовым потерям или нанесению урона репутации организации.

В целом, киберучения среди сотрудников являются важным инструментом для укрепления информационной безопасности организации и подготовки персонала к действиям в мире, где киберугрозы становятся все более распространенными и утонченными.

Для проверки знаний и уровня осведомленности сотрудников казахстанских организаций команда «STS» использует различные инструменты для эмуляции кибератак, таких как фишинговые сообщения и интернет-ресурсы, а также эмуляции различных типов вредоносных вложений. Данные мероприятия проводятся по согласованию с организациями, чтобы оценить реакцию и готовность сотрудников к отражению подобных инцидентов информационной безопасности.

Стоит также отметить, что команда «STS» принимает обращения от пользователей через различные каналы, такие как:

Telegram-канал
«Информационная безопасность РК»
t.me/kzcert

Бесплатный
call-центр
1400

Telegram-бот
«KZ-CERT BOT»
t.me/KZ_CERT_chat_bot
Был разработан для автоматизации подачи заявок от пользователей, а также для отслеживания статусов обработки заявок в реальном времени.

Формы **«Сообщить об инциденте ИБ»**
на официальном интернет-ресурсе
cert.gov.kz
на платформе для обмена информацией об инцидентах ИБ
misp.sts.kz

Электронные почтовые адреса:
incident@cert.gov.kz
info@sts.kz

Цель команды «STS» - не только реагировать на существующие угрозы, но и предупреждать их возникновение путем обучения. Команда «STS» стремится создать культуру информационной безопасности, где каждый член нашего сообщества будет понимать свою роль в обеспечении информационной безопасности и активно участвовать в защите от возможных угроз ИБ.

Рекомендации команды «STS» для реализации цели

Повышайте свою осведомленность об информационной безопасности через участие в образовательных мероприятиях, семинарах и вебинарах. Следите за последними трендами в информационной безопасности и обучайте себя основам безопасного поведения в сети. Также следите за аккаунтами команды в социальных сетях, чтобы оставаться в тренде последний событий по ИБ.

Используйте сильные пароли для своих онлайн-аккаунтов и активируйте двухфакторную аутентификацию, чтобы усилить защиту доступа к своим данным.

Регулярно обновляйте программное обеспечение на своих устройствах, включая операционные системы и антивирусные программы, чтобы исправить уязвимости.

Будьте осторожны при открытии вложений в электронных письмах с переходом по подозрительным ссылкам и предоставлением личной информации. Не доверяйте непроверенным источникам.

Для пользователей:

Периодически проверяйте свои онлайн-аккаунты на несанкционированный доступ и подозрительную активность.

Установите и регулярно обновляйте антивирусное программное обеспечение на своих устройствах.

Проходите курсы по безопасности в интернете и обучайтесь тому, как распознавать и избегать угрозы ИБ.

Избегайте использования общественных Wi-Fi сетей для выполнения чувствительных операций.

Для сотрудников организаций:

Развивайте активное взаимодействие с IT/ IS-отделом и участвуйте в регулярных тренингах по безопасности, предоставляемых организацией.

Соблюдайте политики безопасности компании, особенно в отношении обработки и передачи конфиденциальной информации.

Поддерживайте актуальными антивирусные программы и программное обеспечение, а также обеспечивайте физическую безопасность рабочих мест сотрудников.

Знайте процедуры реагирования на инциденты ИБ и моментально сообщайте о подозрительной активности или инцидентах своему IT/ IS-отделу.

Регулярный анализ в течение года международных угроз и событий в области информационной безопасности оправдан по ряду ключевых причин. В первую очередь, динамичная природа угроз информационной безопасности требует регулярного мониторинга, так как злоумышленники постоянно совершенствуют свои методы атак. Только систематический анализ поможет выявлять новые угрозы и эффективно реагировать на них.

Глобальный характер Интернета означает, что угрозы в виртуальном пространстве также имеют международные масштабы. Анализ международных угроз позволяет не только понимать общие тенденции, но и выявлять мотивы атак, что является важным компонентом разработки стратегий ***киберзащиты.***

Защита критической инфраструктуры становится все более важной, поскольку многие кибератаки направлены именно на такие объекты, как государственные учреждения, энергетические системы и транспортные сети. Регулярный анализ угроз помогает выявлять и анализировать уязвимости, а также разрабатывать и улучшать меры безопасности.

С ростом объемов цифровой информации и распространением личных данных защита конфиденциальности становится более актуальной. Анализ угроз позволяет выявлять потенциальные угрозы для обработки и хранения личных данных, что необходимо для поддержания высокого уровня безопасности.

В 2023 году в международном сообществе были распространены следующие типы угроз и инцидентов информационной безопасности:

Атаки на конечные точки *Endpoint-Based Attacks*

Атаки на конечные точки представляют серьёзную угрозу для бизнеса во всех отраслях промышленности. Поскольку количество конечных точек увеличивается, а возможности удаленной работы продолжают оставаться нормой, поверхность атаки на конечные точки расширяется и делает организации уязвимыми для целого ряда угроз. В этих атаках использовались уязвимости компьютеров, смартфонов и IoT-устройств *(Интернет вещей)*, включая программы-вымогатели, фишинговые атаки, эксплойты нулевого дня, вредоносные программы без файлов и атаки типа «отказ в обслуживании».

Атаки с использованием программ-вымогателей

Данные атаки были нацелены в основном на критически важные объекты информационно-коммуникационной инфраструктуры и компании.

Наиболее резонансные инциденты:

Система скоростного транспорта в районе залива Сан-Франциско

Vice Society

В январе система BART в Сан-Франциско пострадала от атаки программы-вымогателя, ответственность за которую взяла на себя группа Vice Society. Хотя сбоев в обслуживании не произошло, украденные данные были размещены в Интернете. BART подтверждает отсутствие воздействия на службы или внутренние системы, но инцидент вызвал опасения из-за потенциального бэкдор-доступа к критически важным системам.

Reddit

BlackCat Ransomware

Группа вымогателей ALPHV, также известная как BlackCat, взяла на себя ответственность за февральскую кибератаку на Reddit. Атака, инициированная успешной **фишинговой кампанией, привела к краже 80 ГБ** данных, включая внутренние документы, исходный код, а также информацию о сотрудниках и рекламодателях. Группа объявила о своем намерении раскрыть украденные данные после неудачных попыток вымогать у Reddit 4,5 миллиона долларов за их удаление.

Dole Food Company

Компания Dole Food подтвердила произошедшую в феврале атаку с использованием программы-вымогателя, в результате которой было скомпрометировано нераскрытое количество записей сотрудников. Хотя воздействие было ограниченным, производственные предприятия в Северной Америке были временно закрыты из-за атаки. Инцидент повлиял на данные о рабочей силе Dole, о чем сообщается в ежегодном отчете, подаваемом в SEC.

Служба маршалов США

USMS

В результате атаки программы-вымогателя на Службу маршалов США *(федеральный правоохранительный орган в составе Министерства юстиции)* скомпрометированы конфиденциальные данные правоохранительных органов, включая результаты судебных процессов, административные данные и личные данные. Идентифицируемая информация *(PII)* субъектов, связанных с расследованиями USMS, третьих лиц и некоторых сотрудников USMS.

Город Орегон

Royal Ransomware

В г. Орегон, США в результате атаки программы-вымогателя были зашифрованы данные округа. Электоральный и экстренный сервисы остались под контролем, но все остальные операции правительства были зашифрованы. По заявлению Royal Ransomware, злоумышленники потребовали выкуп за доступ к данным, точную сумму чиновники округа не озвучили.

Enzo Biochem

В апреле биотехнологическая компания из Нью-Йорка подверглась атаке программы-вымогателя, скомпрометировавшей данные испытаний, а также личную информацию примерно 2,5 миллионов человек. Был получен доступ к именам, данным тестов и 600 000 номерам социального страхования. Атака на Enzo последовала за отдельной атакой на фармацевтического гиганта PharMerica в мае, в результате которой были раскрыты конфиденциальные данные почти 6 миллионов человек.

Программы-вымогатели ESXi и Linux

Различные группы программ-вымогателей продолжали атаковать серверы VMware ESXi и системы Linux, нарушая работу критически важных служб и данных.

Национальная комиссия по ценным бумагам Аргентины стала жертвой кибератаки

В июне 2023 года Национальная комиссия по ценным бумагам Аргентины стала жертвой кибератаки, предположительно совершенной хакерской группировкой Medusa, занимающейся разработкой вирусов-вымогателей.

Хакеры требовали выкуп в размере $500 тыс. в течение недели, угрожая в противном случае разместить в Интернете 1,5 Тб документов и баз данных комиссии, под угрозой утечки находились конфиденциальные файлы и записи, которые потенциально могли потрясти финансовые рынки Аргентины.

По данным Bleeping Computer, вымогательская операция Medusa набрала значительные обороты с начала 2023 года, нацелившись на корпоративных жертв по всему миру с многомиллионными требованиями выкупа. С мая 2023 года хакеры из Medusa активизировали свою деятельность, запустив свой блог. Эта платформа служит для утечки данных жертв, отказавшихся платить выкуп, что привлекает к ним повышенное внимание СМИ.

Группа вымогателей Medusa в мае 2023 года взяла на себя ответственность за атаку на крупный онкологический центр в Австралии, в ходе которой хакеры потребовали выкуп в размере $100 тыс. В апреле 2023 года хакеры

также выложили в Интернет исходный код сервисов Microsoft Bing и Cortana. Вирус-вымогатель Medusa в феврале 2023 года атаковала как минимум 18 организаций по всему миру. Вирус поддерживает множество аргументов, способных изменить принцип его работы. При обычном запуске программное обеспечение автоматически завершает работу более 280 служб и процессов Windows, чтобы ничего не препятствовало шифрованию файлов, затем ищет и удаляет резервные копии ОС, чтобы предотвратить их использование для восстановления файлов.

Операторы программы-вымогателя LockBit заявили, что группировка приняла решение выложить все внутренние файлы, похищенные у корпорации Boeing

Киберпреступники пошли на это после отказа авиастроительного гиганта выплатить выкуп. Согласно информации в X-аккаунте MalwareHunterTeam, операторы LockBit выложили файлы. Обнародованные архивы и резервные копии систем Boeing в общей сложности весят около 50 ГБ. Пресс-секретарь Boeing подчеркнул, что киберинцидент частично затронул производственные процессы Boeing, но тем не менее не представляет никакой опасности для самолетостроения и полётов. Операторы Lockbit добавили Boeing в список жертв на сайте утечек в сети Tor.

Наиболее распространенные штаммы программ-вымогателей, которые наблюдались в вышеописанных инцидентах:

Royal

Киберпреступники атакуют американские и международные организации с помощью программы-вымогателя Royal с сентября 2022 года.
После проникновения в сети они отключают антивирус и крадут данные перед внедрением программы-вымогателя. Инструкции по выкупу поступают после шифрования через URL-адрес .onion и требуют различных сумм от 1 до 11 миллионов долларов в биткойнах. Было замечено, что программа-вымогатель Royal нацелена на такие важные сектора, как производство, связь, здравоохранение и образование.

LockBit 3.0.

Операции LockBit 3.0 *(также известные как LockBit Black)* следуют модели «программа-вымогатель как услуга» *(RaaS)* и являются более уклончивым и модульным продолжением своих предшественников LockBit и LockBit 2.0.

Было замечено, что филиалы, использующие LockBit 3.0, эксплуатируют различные TTP для атак на широкий спектр предприятий в критически важных секторах инфраструктуры.

BianLian

BianLian – это группа киберпреступников, которая с июня 2022 года проводит атаки с использованием программ-вымогателей на критически важную инфраструктуру США и Австралии.

Известные разработкой, внедрением и вымогательством данных программ-вымогателей, они часто используют для разведки действительные учетные данные протокола удаленного рабочего стола *(RDP)*, а также инструменты с открытым исходным кодом, а для извлечения данных используют FTP, Rclone или Mega. В 2023 году BianLian перешел от использования модели двойного вымогательства к вымогательству на основе эксфильтрации, угрожая раскрыть данные, если выкуп не будет выплачен. В предыдущих кампаниях они были нацелены на сектор профессиональных услуг и развития недвижимости.

Cl0p

С момента своего появления в феврале 2019 года CL0P развивалась и теперь функционирует как Ransomware-as-a-Service *(RaaS)*, продавая доступ к взломанным сетям.

Первоначально известные своим двойным вымогательством, в 2021 году они изменили тактику и сосредоточились на краже данных. Cl0p скомпрометировал более 3000 организаций в США и 8000 организаций по всему миру. В мае 2023 года группа вымогателей Cl0p *(также известная как Clop)* произвела фурор, воспользовавшись уязвимостью нулевого дня в приложении сервера передачи файлов MOVEit, которое работает на серверах Windows. Цепочка эксплойтов доставляет веб-оболочку Microsoft Internet Information Services *(IIS)* .aspx в каталог \MOVEitTransfer\wwwroot\ сервера, которая крадет файлы с сервера, а также из подключенного хранилища BLOB-объектов Azure.

В отчете SentinelOne представлены запросы, которые организации могут использовать для выявления потенциальных атак со стороны группы Cl0p. Атака продемонстрировала значительный сдвиг: традиционно ориентированные на конечные точки злоумышленники-вымогатели написали код специально для служб облачного хранения. Воздействие было огромным: более 500 организаций и данные 34 миллионов человек были скомпрометированы, что сделало эту кампанию одной из крупнейших угроз 2023 года.

QakBot

Также известный как Qbot, Quackbot, Pinkslipbot и TA750, Qakbot с 2008 года вызывал многочисленные глобальные заражения вредоносным ПО. Первоначально это был банковский троян, но он превратился в универсальный вариант ботнета и вредоносного ПО, используемого для разведки, кражи данных, горизонтального перемещения и доставки программы-вымогателя. QakBot нацелен на различные секторы, включая финансовые и аварийные службы, коммерческие объекты, а также подсектор электоральной инфраструктуры, продавая доступ к скомпрометированным устройствам для дальнейших целей аффилированных злоумышленников.

Атака на цепочку поставок 3CX

В ходе обнаруженной атаки на цепочку поставок, получившей название «SmoothOperator», субъекты, связанные с северокорейским режимом, скомпрометировали инфраструктуру платформы 3CX Private Automatic Branch Exchange *(PABX)*.

Компания по разработке программного обеспечения VoIP используется более чем 600 000 человек по всему миру и имеет более 12 миллионов ежедневных пользователей, включая организации из автомобильной промышленности, пищевой промышленности, гостиничного бизнеса, поставщиков услуг управляемых информационных технологий *(MSP)* и обрабатывающей промышленности.

Злоумышленники использовали этот доступ для внедрения вредоносного кода в клиенты конечных точек 3CX, который загружался жертвами в виде обновлений. В версии с бэкдором применялась скрытая стеганография путем кодирования заглушки полезной нагрузки в файле изображения .ico, размещенном в общедоступном репозитории кода, расположенном по адресу github[.]com/IconStorages/images, что позволяло вредоносному ПО получить адрес активного сервера C2.

Утечка данных
Data leak

Атака на Capita

В марте 2023 года компания Capita, один из крупнейших поставщиков аутсорсинговых услуг, столкнулась с серьёзной кибератакой. Этот инцидент привёл к компрометации внутренних систем компании, включая приложения Microsoft Office 365.

В результате атаки были затронуты данные множества клиентов Capita, среди которых были местные власти, государственные организации, включая Британскую армию и Национальную службу здравоохранения *(NHS)*, BBC, а также данные около 470 000 членов крупнейшего университетского пенсионного фонда в Великобритании.

Атака на WH Smith

В марте 2023 года WH Smith, известная торговая марка в Великобритании, столкнулась с кибератакой, которая привела к утечке конфиденциальных данных сотрудников. В результате атаки были скомпрометированы имена, адреса, национальные страховые номера и даты рождения текущих и бывших сотрудников.

Благодаря тому, что клиентские аккаунты хранились в отдельной системе, они остались незатронутыми. WH Smith немедленно уведомил Лондонскую фондовую биржу об инциденте и предпринял меры по укреплению системы безопасности.

Утечка данных 37 млн абонентов

19 января 2023 года стало известно о том, что данные около 37 млн. абонентов американского сотового оператора T-Mobile были похищены хакерами. Системы оператора подверглись хакерской атаке еще в ноябре 2022 года, но известно об этом стало лишь в январе 2023 года.

Злоумышленникам удалось получить доступ к личным данным абонентов, включая даты рождения, телефонные номера и адреса. При этом пароли, секретные коды, банковская информация, а также данные из государственных документов оказались нетронутыми. С помощью внешних экспертов по кибербезопасности оператор мобильной связи T-Mobile остановил утечку на следующий день, сообщила компания.

Киберпреступники получили доступ к информации о кредитных картах клиентов авиакомпании Air Europa

10 октября 2023 года Air Europa отправила клиентам письма о том, что в результате кибератаки злоумышленники могли получить доступ к их платежным данным.

Известно, что киберпреступники получили доступ к номерам кредитных карт, срокам их действия и CVV/CVC. При этом хранение кодов CVV/CVC противоречит правилам стандарта безопасности данных платежных карт *(PCI DSS)*. Представители компании сообщили, что 28 августа специалисты обнаружили подозрительную активность во внутренних системах.

Пострадавших клиентов авиакомпания проинформировала о случившемся инциденте лишь 41 день спустя. Air Europa заявляет, что у нее нет подтвержденных случаев мошенничества с украденными данными, но при этом призывает клиентов аннулировать кредитные карты, если они использовались для оплаты билетов.

Атака на ChatGPT Plus

В марте 2023 года сервис ChatGPT Plus от OpenAI столкнулся с серьёзной утечкой платёжных данных подписчиков. Проблема была вызвана уязвимостью в одной из используемых библиотек.

В результате этой уязвимости, в течение девяти часов, некоторые пользователи могли видеть платёжные данные других пользователей, включая имена, адреса электронной почты, платёжные адреса, последние четыре цифры номеров кредитных карт и сроки их действия. OpenAI быстро устранила проблему и уведомила пользователей о произошедшем.

Несанкционированный доступ
Кибератаки

4 порта в Австралии остановили работу из-за кибератаки

10 ноября 2023 года компания DP World, крупнейший портовый оператор Австралии, подверглась мощной кибератаке, которая парализовала работу информационной инфраструктуры. DP World управляет 40% контейнерных перевозок Австралии через терминалы в Сиднее, Мельбурне, Брисбене и Фримантле. В результате хакерского вторжения задержано прибытие и отправка более 30 тыс. контейнеров, что, по мнению экспертов, спровоцирует рост цен на самые разные товары в стране.

Атака хакеров на Qulliq Energy

Канада

В середине января 2023 года крупный поставщик электроэнергии в Канаде Qulliq Energy пострадал от кибератаки, в результате которой компьютеры были выведены из строя, а ее клиенты лишились возможности платить за услуги с помощью банковских карт.

Представители компании Qulliq Energy сообщали, что атака началась 15 января 2023 года, и, хотя электростанции продолжили работать в нормальном режиме, компьютерные системы в службе поддержки клиентов и административных офисах корпорации были недоступны. Компания не смогла принимать платежи по кредитным картам, клиенты могли оплачивать счета только наличными или банковскими переводами.

Blind Eagle

5 января 2023 года эксперты Check Point Research (CPR) рассказали об одной из самых сложных цепочек заражения в истории кибератак, которую группировка Blind Eagle использует для организации нападений в Южной Америке. Злоумышленники атакуют испаноязычные цели в Колумбии и Эквадоре.

Пользователю может прийти фишинговое электронное письмо от государственного ведомства Колумбии, в частности Министерства иностранных дел. В нём получателю угрожают проблемами при выезде из страны, если он не решит «бюрократический вопрос». Письма содержат ссылку и PDF-файл, направляющий жертву по той же ссылке. При попытке перехода анализируется входящий HTTP-запрос: если он исходит из-за пределов Колумбии, сервер обрывает цепочку заражения и перенаправляет пользователя на настоящий сайт миграционного отдела МИД Колумбии. Однако если запрос поступает из Колумбии, атака продолжается.

Взлом сотрудника биржи с помощью SMS-атаки

17 февраля 2023 года криптовалютная биржа Coinbase сообщила о кибератаке, нацеленной на одного из её сотрудников. Неизвестный злоумышленник украл учётные данные для входа в систему работника Coinbase, пытаясь получить удалённый доступ к ИТ-инфраструктуре компании.

По информации Coinbase атака началась 5 февраля 2023 года: злоумышленник разослал нескольким сотрудникам Coinbase SMS-сообщения с призывом войти в учётные записи своей компании для получения некоего важного уведомления.

Один из сотрудников попался на уловку и перешёл по ссылке, попав на фишинговую страницу, где ввёл свои учётные данные. Затем мошенник попытался войти во внутренние системы Coinbase, используя украденную информацию, но не смог этого сделать, поскольку доступ был защищён многофакторной аутентификацией. Не получив доступ к системе, киберпреступник позвонил тому же сотруднику криптовалютной биржи, представившись ИТ-специалистом Coinbase. Злоумышленник убедил сотрудника войти на свою рабочую станцию и выполнить некоторые действия.

Команда безопасности CSIRT Coinbase в течение 10 минут обнаружила подозрительную активность и оперативно связалась с сотрудником, который поняв, что стал жертвой мошеннической схемы, прервал связь со злоумышленником.

Масштабная SEO-атака через WordPress

В феврале 2023 года злоумышленники осуществили значительную кибератаку на сайты, работающие на системе управления содержимым сайта «WordPress». Целью атаки было манипулирование поисковой оптимизацией (SEO). Злоумышленники использовали уязвимости в WordPress для внедрения вредоносных рекламных объявлений на целевые сайты.

Эти объявления перенаправляли посетителей на поддельные страницы с вопросами и ответами. Поддельные страницы были созданы для улучшения SEO-позиций сайтов злоумышленников. При переходе на эти страницы пользователи не только становились жертвами обмана, но и неосознанно помогали злоумышленникам улучшать рейтинг их сайтов в поисковых системах. Это достигалось за счет увеличения трафика и возможно, через использование скрытых SEO-техник на этих страницах.

Таким образом, эта атака была не просто кибервредоносной, но и угрожала целостности и достоверности результатов поисковых систем, что является особенно тревожным в свете растущей зависимости бизнеса и пользователей от поисковых технологий.

Атака на Royal Mail

В январе 2023 года Royal Mail, национальная почтовая служба Великобритании, стала целью кибератаки, осуществленной российской группой LockBit. Этот инцидент серьёзно затруднил их международные почтовые операции, вызвав значительные задержки в доставке посылок и писем за пределы страны.

Национальные почтовые услуги также испытали определенные нарушения. Компания заявила о «киберинциденте». Позже злоумышленники опубликовали данные сотрудников Royal Mail, чтобы усилить давление на компанию в целях выплаты выкупа.

Атака на ABB

В мае 2023 года ABB, ведущая глобальная компания в области автоматизации и энергетики, подверглась кибератаке, инициированной группой Black Basta. В результате этой атаки были скомпрометированы сотни устройств компании, включая компьютеры и серверы. Атака началась с внедрения вредоносного программного обеспечения в Windows Active Directory компании, что позволило хакерам получить доступ к значительному количеству корпоративных данных и систем.

Хакеры использовали техники шифрования для блокировки доступа к важным файлам и системам, ставя под угрозу как внутренние операции, так и клиентскую информацию. Компания была вынуждена временно отключить все VPN-подключения, чтобы предотвратить дальнейшее распространение атаки и защитить оставшиеся системы. Этот инцидент подчеркивает растущую угрозу, которую кибератаки представляют для крупных промышленных и технологических предприятий.

Атака на The Guardian

В конце декабря 2022 и начало января 2023 года ежедневная газета Великобритании The Guardian подверглась сложной фишинговой кампании, которая привела к серьёзному нарушению их внутренних операций. Злоумышленники, используя методы социальной инженерии, обманным путём получили доступные данные от одного из сотрудников.

После этого они смогли проникнуть в сеть издания, получив доступ к конфиденциальной информации. В результате атаки редакция была вынуждена перейти на удалённую работу на два месяца, что значительно усложнило процесс подготовки и выпуска материалов. Среди скомпрометированных данных оказались личные данные сотрудников, включая зарплаты, банковские реквизиты и номера паспортов.

Атака на Lacroix

12 мая 2023 года Lacroix, компания, занимающаяся производством электронных компонентов, столкнулась с критической кибератакой. В результате атаки вирус-шифровальщик зашифровал виртуальную инфраструктуру компании, что привело к серьёзным нарушениям в работе.

В результате были закрыты три из восьми заводов компании на неделю. Эти заводы играли важную роль в общем объеме продаж компании, отвечая примерно за 19% от общего объема продаж за предыдущий год. Это событие подчеркивает растущую угрозу, которую кибератаки представляют для производственных предприятий.

Уязвимости

Microsoft Exchange Online и Azure AD

Летом текущего года стали известны подробности атак на несколько правительственных учреждений США, совершенных китайской группировкой STORM-0558. В ходе атак были нарушены права доступа Microsoft к нескольким компонентам, в том числе к широким областям применения и украденному ключу подписи, что позволило злоумышленникам создавать токены сеансов для служб Microsoft затронутых организаций.

В первоначальных отчетах говорилось, что затронута только Exchange Online, хотя исследователи обнаружили, что уязвимость затронула и другие типы приложений Azure Active Directory, включая все приложения, поддерживающие аутентификацию индивидуальных учетных записей. BingBang — это проблема в областях приложений Azure Active Directory (AD), где конфигурация по умолчанию может предоставлять приложениям нежелательный доступ.

Исследователи обнаружили, что конфигурация «по умолчанию» для многих приложений Azure означает, что любой пользователь Azure AD может получить доступ к приложениям. Чтобы устранить проблемы, описанные в BingBang, организации, использующие аутентификацию Azure AD, должны проверить, какие уровни доступа делегированы приложениям, сосредоточив внимание в первую очередь на конфиденциальных и критически важных приложениях.

SymStealer поставила под удар каждого пользователя Google Chrome

13 марта 2023 года стало известно о том, что команда Imperva Red в конце 2022 года обнаружила в браузере Google Chrome уязвимость, которая отслеживается под идентификатором CVE-2022-3656.

На момент, когда уязвимость была активна, она затрагивала свыше 2,5 миллиардов пользователей Chrome и позволяла злоумышленникам украсть конфиденциальные файлы, такие как криптокошельки и учётные данные облачного провайдера.

Злоумышленник мог создать поддельный веб-сайт, предлагающий, например, услугу криптокошелька. А в процессе создания кошелька попросить скачать на компьютер так называемые «ключи восстановления». Эти ключи на самом деле будут zip-файлом, содержащим символическую ссылку на конфиденциальный файл или папку на компьютере пользователя, например, учётные данные облачного провайдера. Когда пользователь разархивирует и загрузит ключи восстановления обратно на веб-сайт, символическая ссылка будет обработана и злоумышленник получит доступ к нужному конфиденциальному файлу. Пользователь может даже не осознавать, что что-то не так, поскольку веб-сайт может выглядеть вполне законным, а процесс загрузки и выгрузки ключей восстановления - нормальная практика для криптовалютных кошельков.

Google полностью устранила уязвимость символических ссылок в Chrome версии 108. Чтобы защитить свои криптоактивы, важно поддерживать программное обеспечение в актуальном состоянии, избегать загрузки сомнительных файлов или перехода по ссылкам из ненадежных источников.

Облачные кражи информации

На протяжении 2023 года наблюдался постоянный рост распространения облачных инфоворов, которые запрашивают учетные данные у неправильно настроенных или уязвимых облачных сервисов.

Некоторые известные примеры включают в себя: AlienFox – это комплексный инструмент, созданный на основе фрагментов кода Androxgh0st и продаваемый через каналы Telegram. Злоумышленники удаленно запускают модульный набор инструментов на основе Python для работы с открытыми облачными сервисами. AlienFox в первую очередь нацелен на учетные данные, которыми злоумышленники могут злоупотреблять для проведения спам-атак, ключи API и секреты популярных сервисов, включая AWS SES и Microsoft Office 365.

Подробную разбивку целевых сервисов можно найти в полном отчете SentinelLabs. Ответвление того же кода, что и AlienFox, Legion имеет во многом те же функции, ориентированные на спам. Как и AlienFox, Legion распространяется среди покупателей, часто посещающих каналы Telegram.

Систематический анализ международных угроз информационной безопасности приобретает важное значение, предоставляя организациям не только инсайты, но и возможность повысить свою готовность и эффективность в реагировании на возможные инциденты информационной безопасности. Этот подход позволяет поддерживать высокий уровень готовности, а также осведомленности.

Постоянное обновление стратегий и методов в области защиты становится ключевым элементом в устойчивой кибербезопасности. Актуальные данные и аналитика об угрозах обеспечивают организации необходимой информацией для адаптации и усовершенствования своих стратегий. Этот цикл постоянного обновления и анализа создает механизм, который позволяет минимизировать риски, связанные с кибератаками и поддерживать высокий стандарт безопасности в цифровой среде.

Таким образом, регулярный анализ международных угроз становится ключевым инструментом для создания более защищенного киберпространства, где организации могут успешно противостоять постоянно меняющимся вызовам в области кибербезопасности.

Статистика по инцидентам ИБ

Анализируя обработанные инциденты информационной безопасности, команда «STS» стремится выделить основные тренды и особенности, что позволит нам не только извлекать уроки из предыдущих опытов, но и разрабатывать более эффективные стратегии по защите от будущих киберугроз.

Наши статистические данные включают в себя разнообразные аспекты инцидентов и кибератак. Предоставление этих данных призвано демонстрировать не только нашу прозрачность, но и позволяет общественности и нашим партнерам лучше понимать динамику угроз в цифровом пространстве.

Этот процесс предоставления статистики по обработанным инцидентам ИБ важен для повышения осведомленности, как внутри команды «STS», так и среди наших заинтересованных сторон. Мы стремимся создать прочный фундамент для будущих исследований, анализа и совершенствования наших стратегий ИБ на основе реальных сценариев и вызовов, с которыми мы сталкиваемся.

С января 2023 года командой «STS» было зарегистрировано более **35 тысяч заявок** по угрозам и инцидентам информационной безопасности.

ВПО 21 940

Наиболее распространёнными типами ВПО в МИО за текущий год стали:

- Malicious-url - **5 277**
- HTTP2.RST_STREAM.Rapid.Reset.DoS - **2 885**
- TCP.Split.handshake - **1 316**
- HTTP2.RST_STREAM.Rapid.Reset.DoS.Rate - **354**
- Memcached.try_read_command_binary.Stack.Buffer.Overflow - **185**

Наиболее распространёнными типами ВПО в ГО за текущий год стали:

- Malicious-url - **1 517**
- HTTP2.RST_STREAM.Rapid.Reset.DoS - **492**
- TCP.Split.handshake - **222**
- HTTP2.RST_STREAM.Rapid.Reset.DoS.Rate - **126**
- Expat.Libexpat.XML.Paser.DOS - **76**

ТОП-5 ГО

По количеству событий, связанных с ВПО:

- МВД РК - **493**
- МФ РК - **414**
- МЦРИАП РК - **396**
- ЦИК РК - **231**
- МЧС РК - **189**

Ботнет
4 040

Наиболее распространёнными типами ботнета в МИО за текущий год стали:

- Mozi.botnet - **1 036**
- njRAT.Botnet - **304**
- Andromeda.botnet - **303**
- Lethic.Botnet - **267**
- Mariposa.Botnet - **217**

Наиболее распространёнными типами ботнета в ГО за текущий год стали:

- Mozi.botnet - **200**
- Lethic.Botnet - **66**
- njRAT.botnet - **66**
- andromeda.Botnet - **63**
- AAEH.Botnet - **35**

ТОП-5
ГО

По количеству событий, связанных с ботнетами:

- МЦРИАП РК - **130**
- МВД РК - **109**
- МЧС РК - **36**
- МСХ РК - **30**
- МФ РК - **28**

Эксплуатация уязвимости – 2 726 инцидентов ИБ

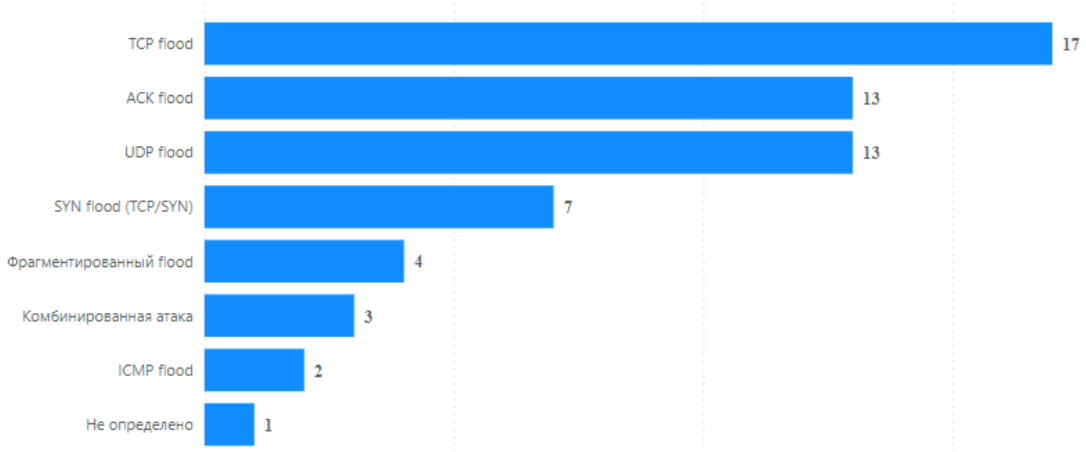
Фишинговая атака – 2 160 инцидентов ИБ

Типы имитации фишинга:

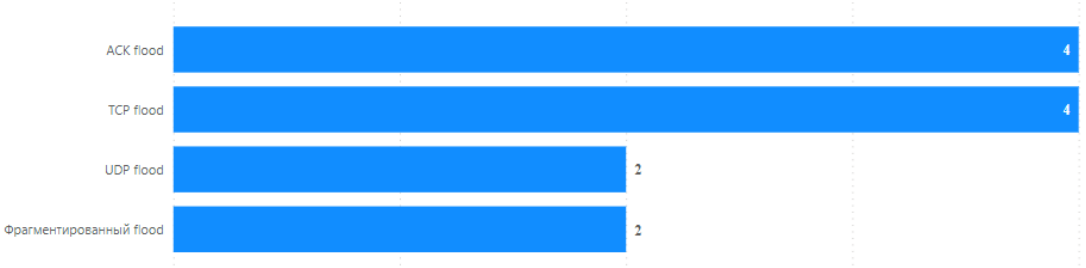
Наименование ИР	Количество фиксаций недоступности	Общее время недоступности *дней*	Общее время недоступности *час*
spon.energo.gov.kz	10	48,3	1 161
pkrezerv.gov.kz	2	25,8	620
election.gov.kz	67	16,1	388
sud.gov.kz	154	14	337
dot.saylau.kz	24	12,3	295

С начала 2023 года зафиксировано **272** события, связанных с **DDoS – атаками.**

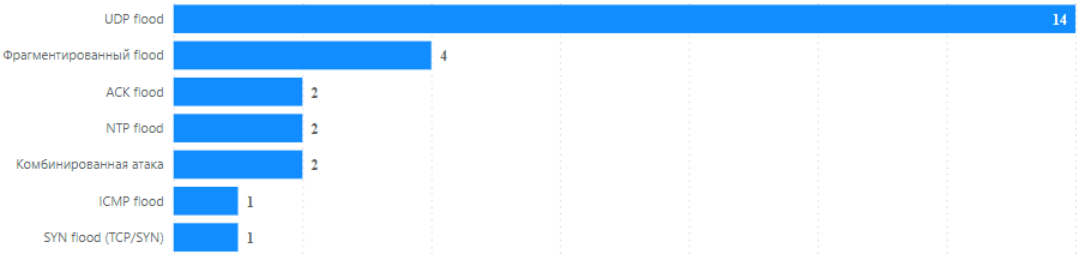
Типы DDoS – атак, направленных на БВУ РК:



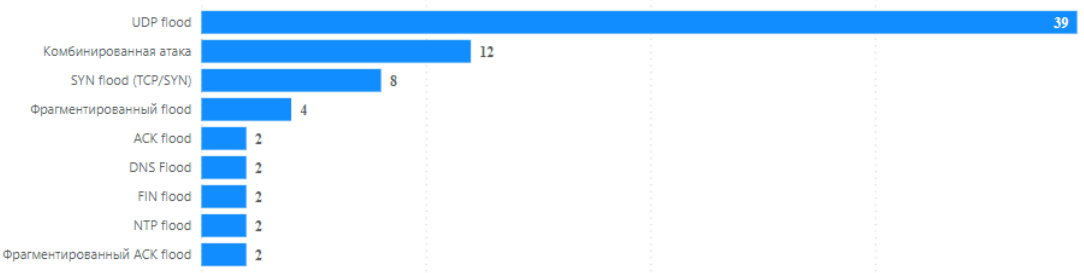
Типы DDoS – атак, направленных на ГО РК:



Типы DDoS – атак, направленных на Квазигосударственный сектор:



Типы DDoS – атак, направленных на КВОИКИ:



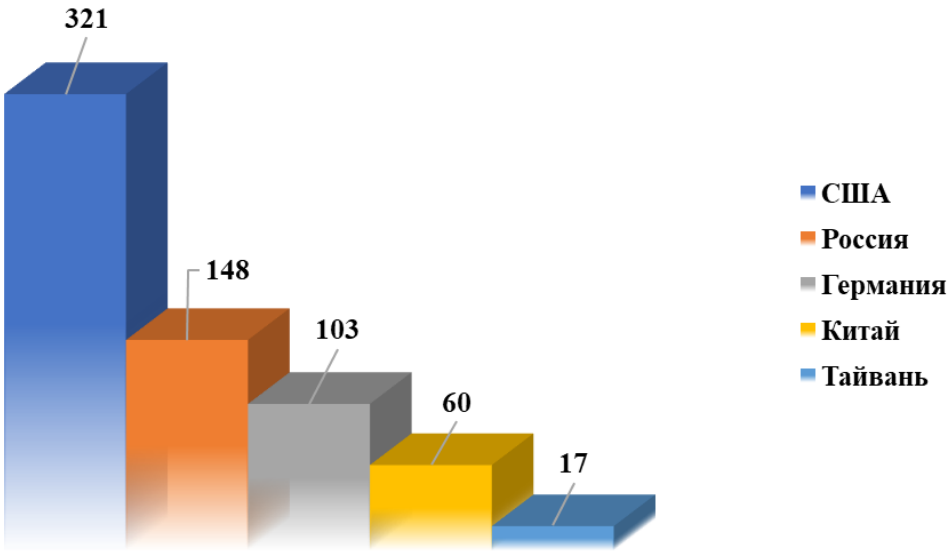
Хотелось бы отметить, что из **272** событий, зарегистрировано и отработано **152** инцидента.

Мероприятия по международному обмену информацией в части выявленных угроз информационной безопасности и компьютерных инцидентов:

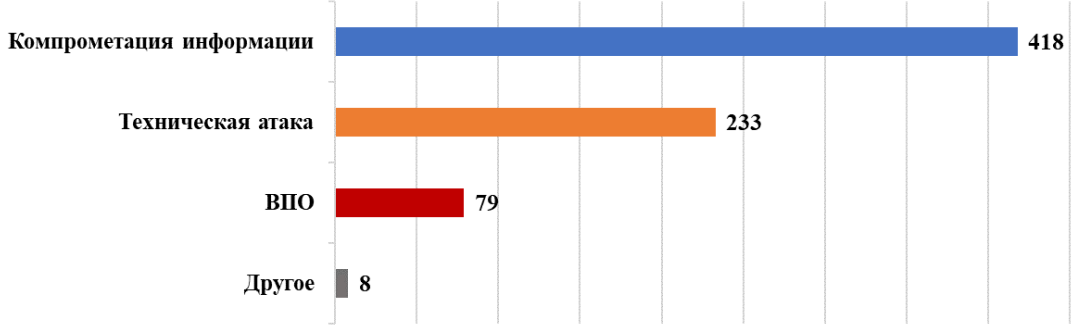
В 2023 г. по результатам отработки событий и инцидентов ИБ НКЦИБ в зарубежные организации **78** государств направлено **1832** оповещения *(сведения, полученные с оборудования Единого шлюза доступа к Интернету и Единого шлюза электронной почты (IPS/IDS).*

Со стороны зарубежных организаций **32** государств в адрес НКЦИБ поступило **738** оповещений.

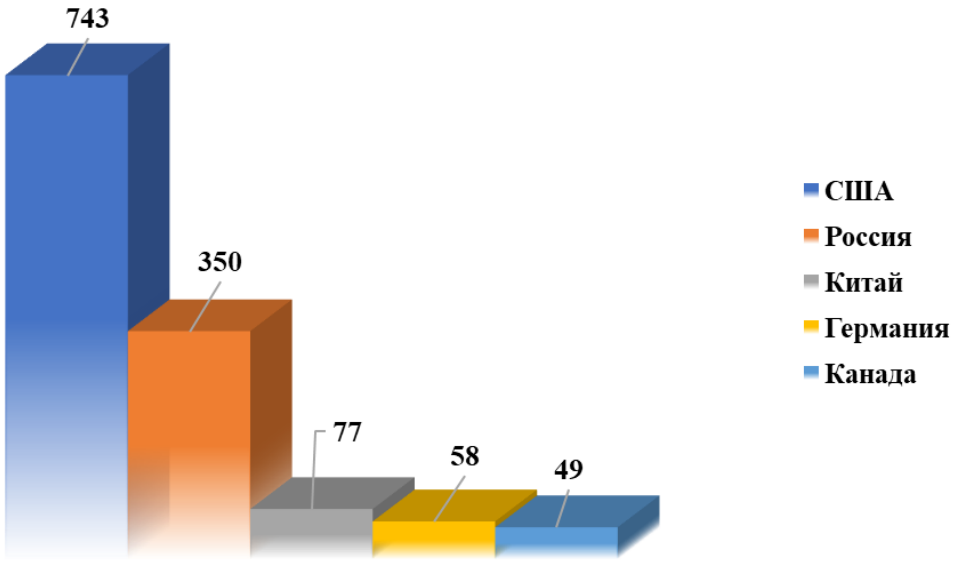
Количество входящих международных оповещений за 2023 г. в разрезе стран (ТОП-5):



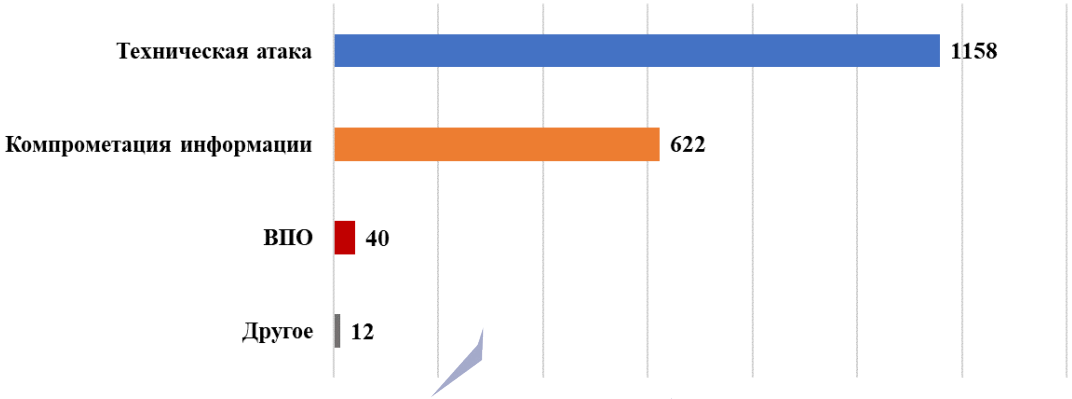
Количество входящих международных оповещений за 2023 г. в разрезе категорий событий/угроз/инцидентов ИБ:



Количество исходящих международных оповещений за 2023 г. в разрезе стран (ТОП-5):



Количество исходящих международных оповещений за 2023 г. в разрезе категорий событий/угроз/инцидентов ИБ:

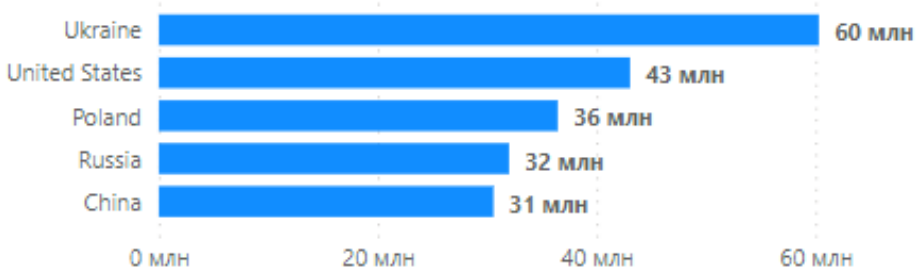


Сведения об атаках на клиентов ЕШДИ

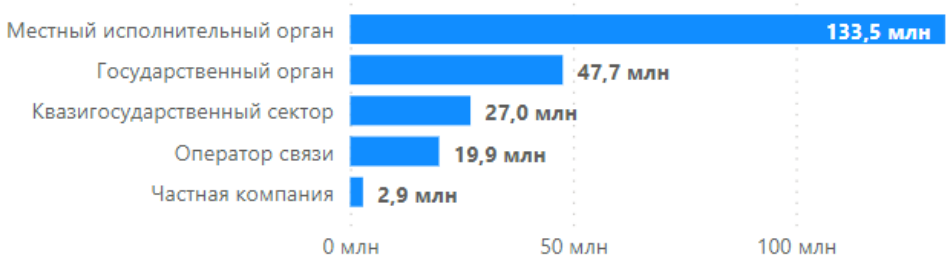
В 2023 году количество попыток найти брешь в защите клиентов ЕШДИ зафиксированы с использованием инфраструктуры стран, указанных в графиках.

Сведения о вредоносной активности, направленной на клиентов ЕШДИ с целью эксплуатации уязвимости CVE-2023-28771 за 2023 год – более 223 млн атак:

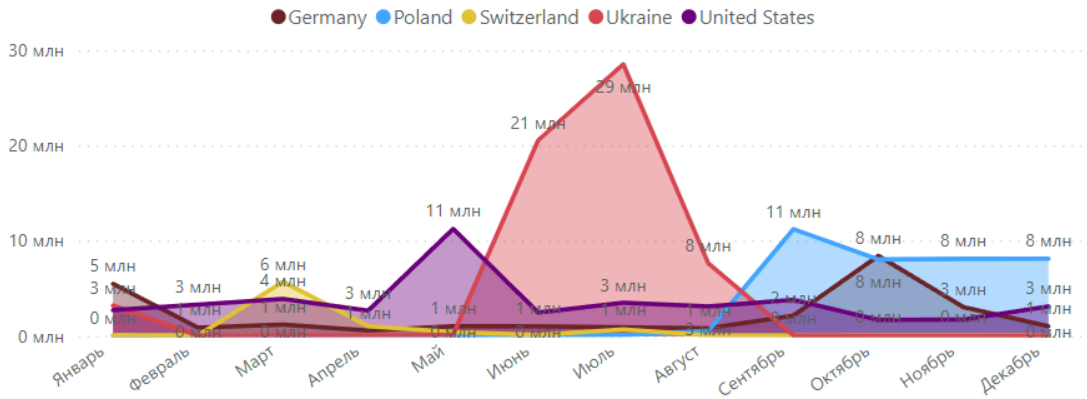
ТОП-5 атакующих стран



ТОП-5 секторов, куда были направлены атаки



Динамика изменения количества атак, исходящих от ТОП-5 атакующих стран

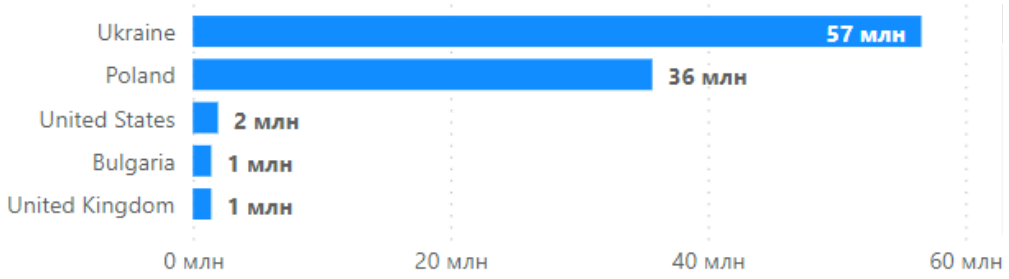


С информацией об уязвимости можно ознакомиться по ссылке: *https://www.fortiguard.com/encyclopedia/ips/53203.*

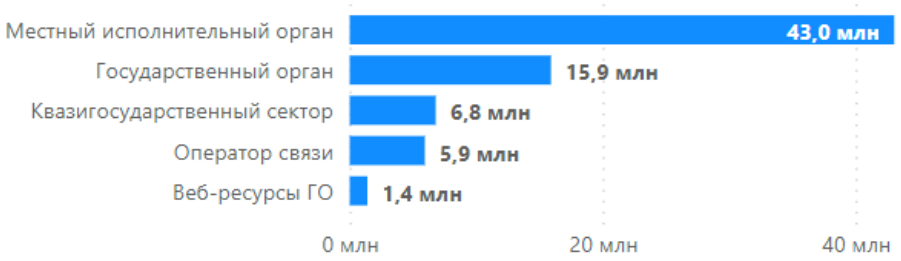
По сведениям Forti, уязвимость затрагивает оборудования Zyxcel, используемые для защиты промышленных систем *(SCADA -Supervisory Control And Data Acquisition).* Доля атаки, которая была направлена на госсектор *(МИО-44%, ГО-18%)*, составила 62%. Атаки преимущественно были направлены на северные регионы РК *(Северо-Казахстанская область, Акмолинская область, Костанайская область).*

Сведения о вредоносной активности, направленной на клиентов ЕШДИ – ТОП-5 атакующих (с использованием инфраструктуры) стран:

ТОП-5 атакующих стран

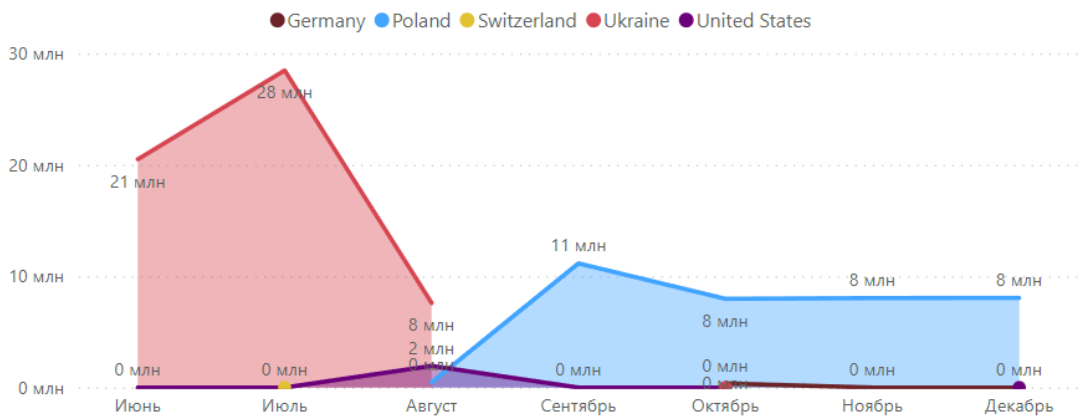


ТОП-5 секторов, куда были направлены атаки



Угрозы

Динамика изменения количества атак, исходящих от ТОП-5 атакующих стран

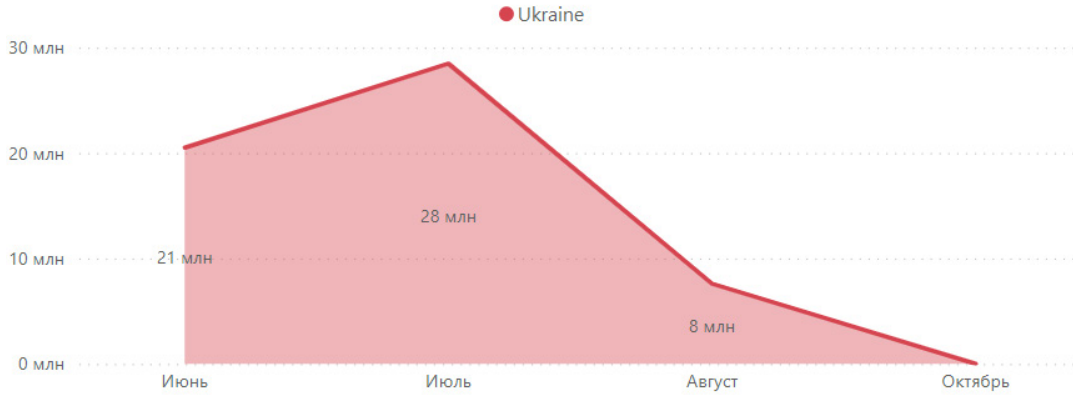


ТОП-3 атакующие страны: с использованием инфраструктуры Украины

Сведения по секторам, куда направлена вредоносная активность

Угрозы

Статистика по месяцам

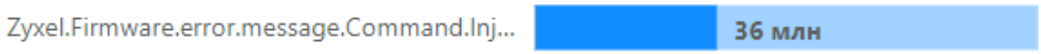


ТОП-5 регионов РК, куда были направлены атаки

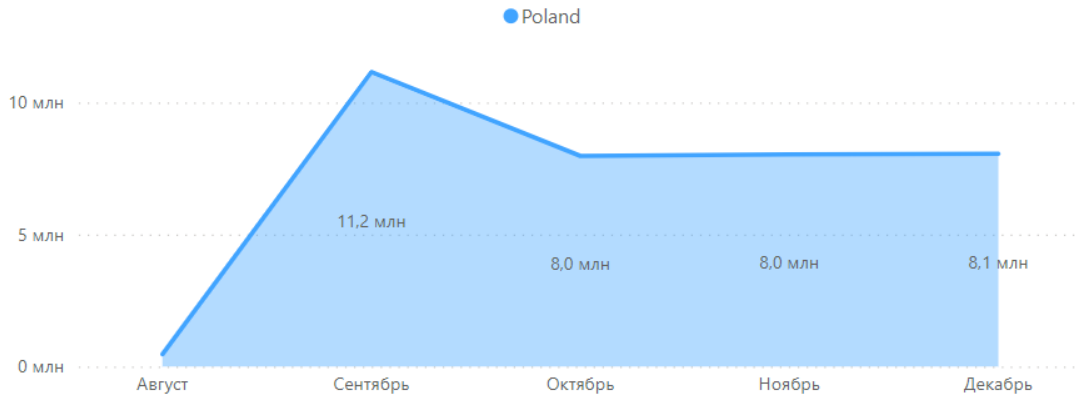
ТОП-3 атакующие страны: с использованием инфраструктуры Польши

Сведения по секторам, куда направлена вредоносная активность

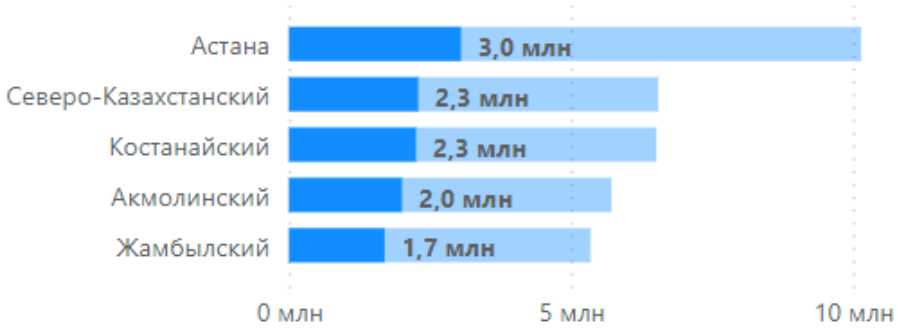
Угрозы



Статистика по месяцам



ТОП-5 регионов РК, куда были направлены атаки

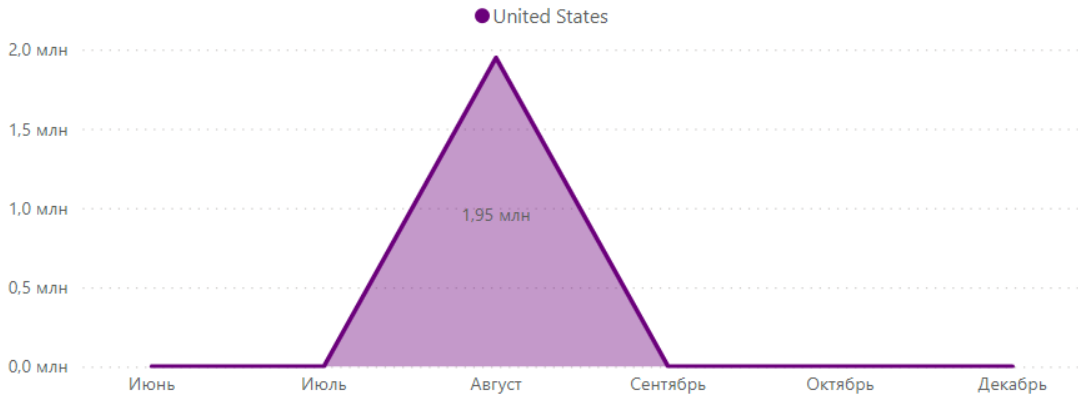


ТОП-3 атакующие страны: с использованием инфраструктуры США

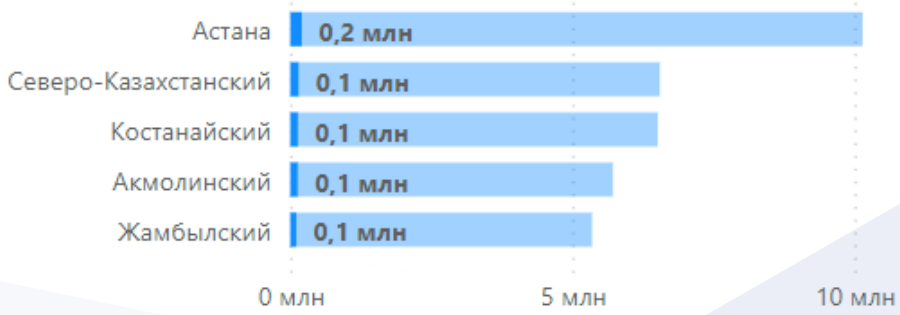
Сведения по секторам, куда направлена вредоносная активность

Угрозы

Статистика по месяцам



ТОП-5 регионов РК, куда были направлены атаки



Команда «STS» активно проводит анализ актуальных уязвимостей в области информационной безопасности и эксплойтов, затрагивающих различные объекты информатизации по всей стране. Эта практика направлена на обеспечение безопасности обычных граждан и защиты их цифрового пространства.

Анализ уязвимостей позволяет нам оперативно выявлять потенциальные слабые места в системах и программных продуктах, которые могут быть использованы злоумышленниками для несанкционированного доступа или атак. Следя за актуальными угрозами, мы предоставляем рекомендации и советы по устранению выявленных проблем, чтобы повысить уровень информационной безопасности как на уровне общественных ресурсов, так и на уровне индивидуальных веб-сайтов.

Наша цель - сделать информацию об угрозах информационной безопасности более доступной и понятной для всех. Мы стремимся предоставить обычным гражданам информацию и инструменты, которые помогут им защитить свою конфиденциальность и безопасность в цифровом мире. Актуальные рекомендации и анализы эксплойтов призваны служить своего рода «цифровым щитом», который обеспечит нашему обществу более высокий уровень информационной безопасности и уверенности в онлайн-пространстве.

Ниже приведены наиболее актуальные уязвимости и эксплойты, которые были применимы для казахстанских объектов информатизации:

GeoServer CVE-2022-24816 и CVE-2023-25157

Национальной службой реагирования на компьютерные инциденты KZ-CERT обнаружены IP-адреса, использующие GeoServer, потенциально подверженные критическим уязвимостям с идентификаторами CVE-2022-24816 и CVE-2023-25157.

GeoServer - открытое программное обеспечение для публикации и обработки геопространственных данных. Оно поддерживает множество форматов для обмена данными, включая WMS *(Web Map Service)*, WFS *(Web Feature Service)*, WCS *(Web Coverage Service)* данных и протоколов, обеспечивая совместимость с другими приложениями GIS *(Geographic information system)*. GeoServer используется в различных отраслях, таких как геология, экология, геодезия, сельское хозяйство, управление городами и др., где пространственные данные являются важными компонентами для принятия решений.

CVE-2022-24816 JAI-EXT - проект с открытым исходным кодом, целью которого является расширение API Java Advanced Imaging *(JAI)*. Программы, позволяющие предоставлять скрипт Jiffle через сетевой запрос, могут привести

к удаленному выполнению кода, поскольку скрипт Jiffle компилируется в Java-код через Janino и выполняется.

В частности, это затрагивает проект GeoServer. CVE-2023-25157 в ряде функций и фильтров при использовании с определенными хранилищами данных, такими как PostGIS и Oracle, были обнаружены уязвимости SQL-инъекций. Эти уязвимости включают фильтр PropertyIsLike, strEndsWith, strStartsWith, фильтр FeatureId, функцию jsonArrayContains и фильтр DWithin. Эти уязвимости потенциально могут быть использованы для получения несанкционированного доступа к системе.

Обнаруженный веб-шелл на интернет-ресурсе kvant.edu.kz

Национальной службой реагирования на компьютерные инциденты KZ-CERT обнаружен веб-шелл на интернет-ресурсе kvant.edu.kz. Веб-шелл *(web-shell)* — это вредоносный скрипт, который может быть загружен злоумышленниками на веб-сервер для удаленного администрирования и выполнения команд. Зараженные веб-серверы могут быть как в сети Интернет, так и во внутренней сети. Это зависит от того, где веб-шелл используется для дальнейшего подключения к внутренним хостам. Веб-шелл может быть написан на любом языке, который поддерживает целевой веб-сервер.

Наиболее частые веб-шеллы написаны на языках, которые широко поддерживаются, таких как PHP и ASP. Также используются сценарии оболочки Perl, Ruby, Python и Unix. Возможности веб-шелла включают в себя работу на PHP версии 4.1.0 и выше, а также использование асинхронных запросов, подобных AJAX. Этот инструмент может использовать методы запросов POST и GET и обфусцировать их, а также работать в пользовательском окружении.

Он поддерживает 22 различных набора символов и шифрует исходный код с помощью вашего ключа (пароля) при загрузке, но не содержит этот ключ в полученном файле. Кроме того, веб-шелл имеет скрытый режим и позволяет работать с различными задачами без перезагрузки страницы и потери данных.

MikroTik RouterOS CVE-2023-30799

Национальной службой реагирования на компьютерные инциденты KZ-CERT в ходе мониторинга казахстанского сегмента Интернета обнаружены IP-адреса клиентов ЕШДИ, использующие MikroTik RouterOS с паролями по умолчанию и подверженные высокому уровню критичности уязвимости идентификатора CVE-2023-30799.

Уязвимость CVE-2023-30799 позволяет повысить привилегии до «Super Admin» через Winbox или HTTP-интерфейсы устройства, используя учетную запись администратора. В отличие от учетной записи admin, которая предоставляет ограниченные привилегии, Super Admin дает полный доступ к операционной системе RouteOS. При повышении привилегий до уровня «Super Admin» можно получить путь к коду, позволяющий контролировать адрес вызова функции.

Уязвимость CVE-2023-3519C Citrix NetScaler ADC и NetScaler Gateway

Национальной службой реагирования на компьютерные инциденты KZ-CERT были обнаружены IP-адреса, использующие продукты Citrix NetScaler ADC и NetScaler Gateway, потенциально подверженные уязвимости с высоким уровнем критичности идентификатора CVE-2023-3519.

NetScaler Application Delivery Controller *(ADC)* – это программно-аппаратный сетевой контроллер, который обеспечивает балансировку нагрузки на серверы, управление трафиком, шифрование данных и защиту от атак в реальном времени. Он позволяет распределять нагрузку на несколько серверов, обеспечивая равномерное распределение запросов и предотвращая перегрузки. Это повышает производительность и доступность приложений для пользователей.

Citrix NetScaler Gateway — это решение для безопасного доступа к приложениям, которое обеспечивает детализированные средства контроля на уровне приложений и данных и одновременно обеспечивает пользователям возможность удаленного доступа из любого места. Уязвимость позволяет злоумышленнику выполнять произвольный код без авторизации. Для возможности эксплуатации затронутые устройства должны быть сконфигурированы как шлюз (например, виртуальный сервер VPN, ICA Proxy, CVPN, RDP Proxy) или виртуальный сервер аутентификации, авторизации и аудита (AAA) с включенным SAML. Уязвимость возникает при отправке слишком большого количества методов каноникализации или преобразования в сообщении SAML.

Уязвимость CVE-2023-36845 Juniper Networks Junos

Национальной службой реагирования на компьютерные инциденты KZ-CERT были обнаружены 28 IP-адресов, использующих продукты Juniper Networks Junos в интерфейсе J-Web ОС на брандмауэрах серии SRX и коммутаторах EX, потенциально подверженных уязвимости с высоким уровнем критичности идентификатора CVE-2023-36845.

Junos — это операционная система для автоматизации сетевых операции. Операционная система широко используется в сетевом оборудовании, таком как маршрутизаторы и коммутаторы Juniper и она предоставляет множество функций для обеспечения надежной и эффективной работы компьютерных сетей. Junos используется в корпоративных сетях и интернет-провайдерах, чтобы обеспечивать связь между компьютерами и другими устройствами в сети.

J-Web — это графический интерфейс, используемый для настройки устройств Junos. Интерфейс J-Web позволяет отслеживать, настраивать, устранять неполадки и управлять платформой маршрутизации с помощью веб-браузера с поддержкой протокола HTTP или HTTPS. Брандмауэр Juniper серии SRX – это интегрированный брандмауэр и устройство безопасности для сетей, который используется для защиты сетей от несанкционированного доступа,

вирусов, атак из интернета и других угроз. Коммутаторы Juniper серии EX — это высокопроизводительные облачные коммутаторы доступа для уровня распределения/ядра, предназначенные для корпоративных и филиальных сетей, а также центров обработки данных. Коммутаторы серии EX упрощают доступ к проводным сетям.

Уязвимость CVE-2023-36845 позволяет злоумышленникам изменить определенную переменную среды PHP в J-Web ОС Juniper Networks Junos на сериях EX и SRX, которая приведет к частичной потере целостности, предоставляя возможность к созданию цепочки уязвимостей.

Уязвимость CVE-2023-46604 Apache ActiveMQ

Национальной службой реагирования на компьютерные инциденты KZ-CERT были обнаружены уязвимые сервисы обмена сообщениями Apache ActiveMQ, которые подвержены уязвимости с высоким уровнем критичности (CVSS 10 из 10) идентификатора CVE-2023-46604.

Apache ActiveMQ — это система обмена сообщениями с открытым исходным кодом, реализующая Java Message Service (JMS) и поддерживающая различные протоколы, такие как MQTT, AMQP, REST и WebSocket. Эта система используется для асинхронного обмена данными в распределенных системах, обеспечивая их интеграцию, масштабируемость и производительность.

ActiveMQ находит применение в различных сферах, включая финансы, телекоммуникации, здравоохранение и розничную торговлю, для обработки транзакций, управления сетевым трафиком, обмена данными между медицинскими учреждениями и интеграции систем управления товарами и заказами. Уязвимость идентификатора CVE-2023-46604 программной платформы Apache ActiveMQ связана с восстановлением в памяти недостоверных данных. Эксплуатация уязвимости может позволить злоумышленнику, действующему удаленно, выполнить произвольный код, путем создания класса по протоколу OpenWire.

Уязвимость CVE-2023-33466 Orthanc Explorer

Национальной службой реагирования на компьютерные инциденты KZ- были обнаружены IP-адреса сервисов для хранения, извлечения и передачи медицинских изображений в сетях с использованием по протоколу DICOM, которые содержали медицинские сведения и персональные данные граждан РК.

Orthanc Explorer — это веб-интерфейс для управления сервером Orthanc, свободным и открытым сервером DICOM, который используется для хранения, извлечения и передачи медицинских изображений в сетях с использованием протокола DICOM. С помощью Orthanc Explorer пользователи могут просматривать, загружать и удалять сведения пациентов, исследования и изображения, а также осуществлять другие операции управления сервером. В Orthanc

до версии 1.12.0 обнаружена критическая уязвимость с идентификатором CVE-2023-33466, имеющая оценку 8.8 из 10 по шкале CVSS. Эта уязвимость может позволить авторизованному злоумышленнику, имеющему доступ к API Orthanc, перезаписывать произвольные файлы в хранилище. В определенных сценариях развертывания это также позволяет злоумышленнику перезаписать конфигурацию системы, что может быть использовано для осуществления удаленного выполнения кода *(RCE)*.

Кроме того, выявленные IP-адреса, на которых развернуты системы Orthanc, не имеют никакой формы авторизации. На этих системах уязвимость CVE-2023-33466 потенциально представляет собой серьезную угрозу. Отсутствие авторизации делает эти системы полностью открытыми для внешних атак и злоумышленники могут легко эксплуатировать уязвимость для перезаписи файлов и выполнения произвольного кода.

Целевые кибератаки

Команда «STS» продолжает наблюдать за активностью хакерской группировки, которая отслеживается нами как STA-2201. Указанная группировка использует публичные, но малоизвестные эксплоиты, а также компонует фрагменты кода из различных источников между собой, создавая принципиально новый функционал. Кроме того, атакующие перекомпилируют инструменты с открытым исходным кодом, включая из GitHub репозиториев, внося минимальные изменения.

В части закрепления в системе и бокового перемещения по инфраструктуре злоумышленники используют возможности средств удаленного администрирования, а также применяют технику Living off the Land (LotL). Атакующие стремятся получить привилегии SYSTEM, что позволит им взаимодействовать с повышенными привилегиями с элементами инфраструктуры, в том числе контролером домена и почтовым сервером Exchange.

При эксплуатации Microsoft Exchange злоумышленники используют механизм ViewState, который позволяет им запускать произвольный код в случае, если они ранее получили значения параметров «validationKey», «decryptionKey» из конфигурационного файла «web.config». После закрепления на сервере Exchange злоумышленники загружают другой вредоносный код, который позволяет им исполнять команды командной строки и сохранять файлы на диске.

Затем, в зависимости от поставленных целей, злоумышленники устанавливают одну или несколько из следующих вредоносных программ:

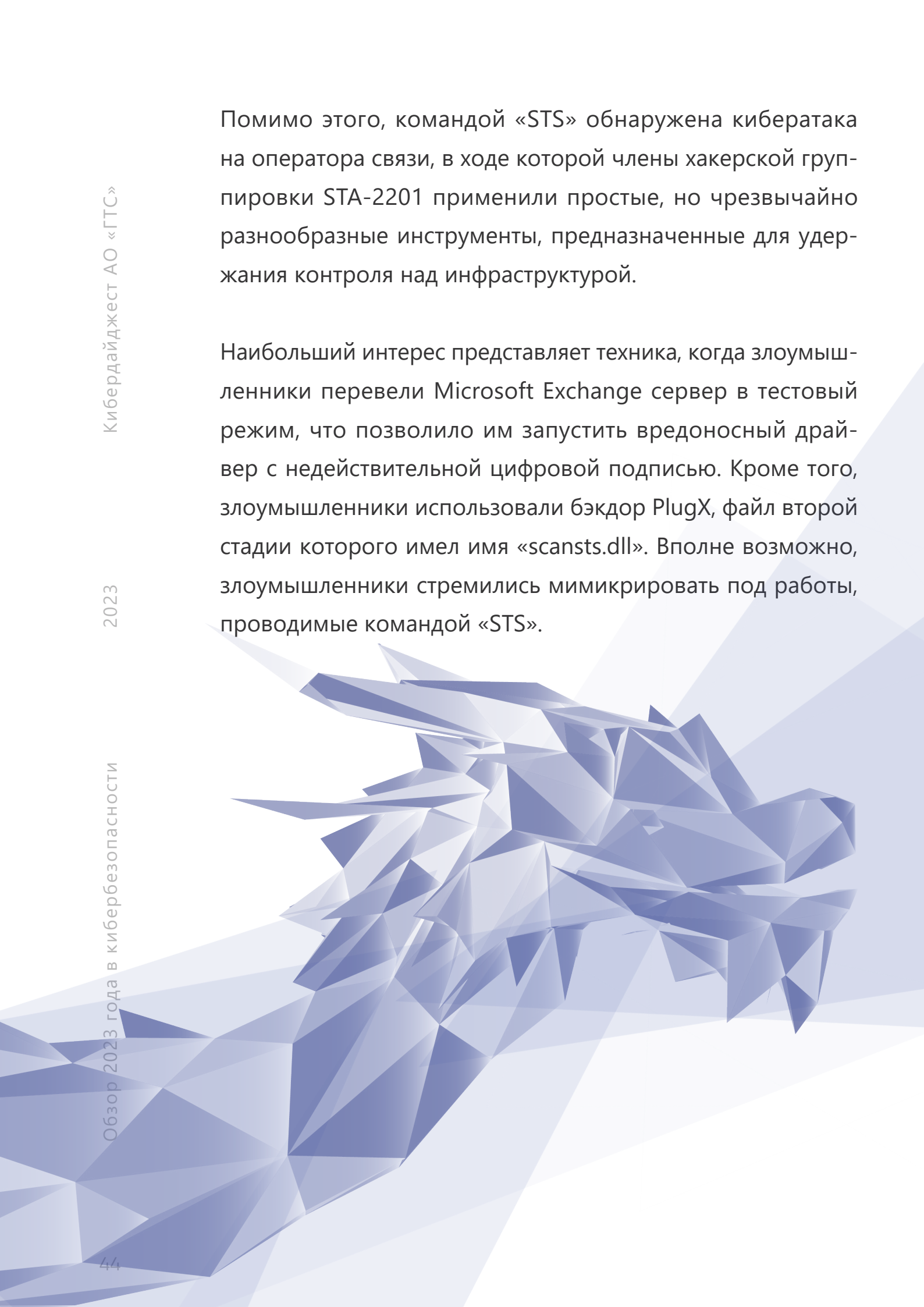
1. Многофункциональный бэкдор PlugX/ShadowPad, который имеет функционал файлового шпиона, клавиатурного шпиона, а также обладает возможностью исполнения команд и загрузки дополнительных вредоносных модулей

2. Бесфайловый бэкдор, который обладает функционалом исполнения команд PowerShell/WMI, файлового шпиона, рекогносцировки в сети, а также совершения атаки типа DCSYNC

3. Установки бэкдора в виде Transport Agent'а, который управляется посредством специально сформированных электронных писем и обладает возможностью исполнения команд и запуска вредоносных модулей

Помимо этого, командой «STS» обнаружена кибератака на оператора связи, в ходе которой члены хакерской группировки STA-2201 применили простые, но чрезвычайно разнообразные инструменты, предназначенные для удержания контроля над инфраструктурой.

Наибольший интерес представляет техника, когда злоумышленники перевели Microsoft Exchange сервер в тестовый режим, что позволило им запустить вредоносный драйвер с недействительной цифровой подписью. Кроме того, злоумышленники использовали бэкдор PlugX, файл второй стадии которого имел имя «scansts.dll». Вполне возможно, злоумышленники стремились мимикрировать под работы, проводимые командой «STS».



Для обеспечения более высокого уровня информационной безопасности рекомендуется использовать комплексный подход, включающий в себя следующее:

1 Организационные меры защиты

Включают в себя законодательные, административные и организационно-технические меры защиты.

Основными источниками законодательных мер защиты являются Закон Республики Казахстан «Об информатизации», Постановление Правительства Республики Казахстан от 20 декабря 2016 года №832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», Нормативные акты Национального банка Республики Казахстан, Закон Республики Казахстан от 31 августа 1995 года № 2444 «О банках и банковской деятельности в Республике Казахстан», Постановление Правления Национального банка Республики Казахстан от 27 марта 2018 года №48 «Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах» и т.д., требования которых должны выполняться организациями в РК.

К административным мерам относятся внутренние документы организаций, направленные на общую координацию действий по защите информации. К таким документам относятся техническая документация по информационной безопасности, управление рисками, планирование действий при ЧС, должностные инструкции и др.

Организационно-технические меры направлены на контроль доступа на территорию, физическую защиту ИС и имущества от повреждений, а также на поддержку работоспособности ИС.

Регулярно актуализируйте техническую документацию по информационной безопасности, анализируйте риски, проводите обучение сотрудников по кибергигиене. Обеспечьте необходимый уровень доступа к объекту информатизации, системам охранной и пожарной сигнализации, системам непрерывного кондиционирования, электроснабжения. Выполняйте резервирование компонентов ИС *(хранение, обработка, передача)*.

2 Программно-технические средства защиты

Включают в себя программные, программно-аппаратные и аппаратные средства защиты.

К ним относятся XDR системы *(антивирус+EDR+SIEM+SPAN)*, межсетевые экраны, DLP системы. Установите надежное антивирусное программное обеспечение на все рабочие станции и серверы в сети организации и регулярно обновляйте его для обнаружения и удаления вредоносных программ, настройте доступы на межсетевых экранах по методу «запрещено все, кроме разрешенного», настройте DLP систему и контролируйте каналы утечки данных.

Необходимо рассмотреть внедрение специализированных решений для обнаружения и предотвращения целенаправленных атак, включая защиту от атак внутри сети. Также необходимо внедрение SIEM/SOAR для анализа и мониторинга событий в реальном времени, обнаружения аномального поведения и реагирования на инциденты информационной безопасности.

3 Криптографические методы защиты

Обеспечьте хранение, передачу важной информации в зашифрованном виде с помощью специализированного ПО. Секретные ключи храните в надежном месте.

4 Средства технической защиты

Предназначены для защиты информации от несанкционированного доступа с использованием средств технической разведки.
Обеспечьте защиту информации с использованием специальных устройств в соответствии с уровнем конфиденциальности информации.

Искусственный интеллект (ИИ) и машинное обучение

В 2024 году ожидается, что развитие ИИ значительно продвинется и принесет с собой множество новых возможностей и вызовов. Стоит также отметить, что одной из главных областей, где ИИ уже демонстрирует себя с большим успехом, является медицина. Врачебные программы на основе ИИ способны диагностировать заболевания с высокой точностью и предлагать оптимальные методы лечения. Это позволяет своевременно обнаружить и бороться с различными заболеваниями, а также повышает эффективность работы медицинских учреждений.

Еще одним направлением, где ИИ обещает революционные изменения, является автоматизация процессов в различных отраслях экономики. С помощью ИИ будет возможно создавать умные системы управления производством, оптимизировать логистические процессы, улучшать качество контроля и многое другое. Это значительно повысит эффективность работы предприятий и позволит снизить затраты.

Применение искусственного интеллекта и машинного обучения в информационной безопасности приносит многочисленные преимущества. Эти технологии обладают способностью улучшать человеческие возможности, проводить быстрый анализ обширных объемов данных, распознавать сложные закономерности и взаимосвязи, а также эффективно адаптироваться к новым угрозам информационной безопасности.

Кроме того, искусственный интеллект и машинное обучение могут автоматизировать рутинные задачи, освобождая специалистов для более глубокого фокусирования на сложных и стратегических задачах. Однако имеются определенные трудности, такие как необходимость в высококачественных и разнообразных данных, ясности и понимании моделей ИИ, возможные атаки со стороны злоумышленников, а также этические вопросы, касающиеся конфиденциальности и предвзятости.

Также одной из главных проблем является этический аспект использования ИИ. Возникают вопросы о приватности данных, безопасности и ответственности за принимаемые ИИ решения. Поэтому важно разработать соответствующие правовые и регуляторные механизмы для обеспечения безопасного и этичного использования ИИ.

В перспективе информационная безопасность искусственного интеллекта, поддерживаемая машинным обучением, станет «мощным» инструментом. Как и во многих других отраслях, человеческое взаимодействие давно уже играет ключевую и неотъемлемую роль в обеспечении безопасности. Несмотря на то, что на данный момент эффективность информационной безопасности в значительной степени зависит от человеческого участия, стоит отметить, что технологии все более успешно справляются с определенными задачами по сравнению с человеческими возможностями.

Генеративный ИИ используется по обе стороны битвы

Поскольку искусственный интеллект развивается ускоренными темпами, растет обеспокоенность по поводу распространения все более сложных и интеллектуальных атак, управляемых искусственным интеллектом.

Спектр угроз включает в себя «дипфейковые» попытки социальной инженерии, а также автоматизированные вредоносные программы, которые демонстрируют интеллектуальное поведение, позволяющее обойти обнаружение различными средствами защиты.

Одновременно эта технология поможет выявлять, избегать или минимизировать потенциальные риски за счет использования обнаружения аномалий в реальном времени, интеллектуальной аутентификации и механизмов автоматического реагирования на инциденты информационной безопасности.

Защита критически важной инфраструктуры

Кибератаки на критически важные инфраструктуры, такие как энергетические сети, транспортные системы и финансовые учреждения представляют собой значительную угрозу национальной безопасности и экономике. В 2024 году ожидается усиление мер по защите этих систем.

Это может включать развитие специализированных решений для обнаружения и предотвращения атак, укрепление сотрудничества между государственными и частными организациями, а также повышение уровня готовности к инцидентам в критических отраслях.

Фишинг

Из-за своей способности манипулировать человеческой психологией фишинговые атаки и атаки социальной инженерии продолжают оставаться эффективными.

Фишинговые атаки включают в себя использование электронных писем или веб-страниц с целью обмана пользователей. Ожидается, что в течение следующих двенадцати месяцев эти атаки станут более изощренными, целенаправленными и убедительными.

Злоумышленники могут использовать технологию глубокой подделки, чтобы выдавать себя за доверенных лиц или манипулировать видео/аудио контентом, что еще больше затрудняет отличить подлинный контент от подделки.

Осведомленность и обучение сотрудников основам информационной безопасности является важной тактикой, которую можно использовать для борьбы с угрозой фишинга.

Кибератаки на устройства IoT

Интернет вещей *(IoT)* является одной из наиболее всеобъемлющих технологий, существующих в настоящее время. Благодаря расширению интернет-сети, увеличению пропускной способности и разнообразию удобных умных устройств, IoT переживает необычайно быстрый рост популярности по всему миру.

Прогнозируется, что в 2024 году темпы роста популярности IoT будут продолжать увеличиваться. IoTпредставляет собой крайне удобный и полезный комплекс технологий, который значительно облегчает как повседневную жизнь, так и операционную деятельность организаций. Тем не менее, увы, идеальных технологий не существует. Несмотря на огромную популярность и удобство устройств IoT, они обладают своими недостатками, такими как наличие трудно выявляемых уязвимостей и отсутствие стандартизации. Устройство IoT является потенциально уязвимой точкой входа в сеть. Поэтому эти сети могут представлять собой первый этап в масштабных взломах, особенно когда атака направлена против конкретной организации.

Основные элементы системы Интернета вещей довольно подвержены атакам со стороны злоумышленников. Независимо от масштаба и типа окружающей среды, в которую внедряется система IoT, безопасность следует рассматривать на этапе проектирования для улучшения ее внедрения, защиты данных и предотвращения кибератак.

Облачная безопасность

Переход на облачные технологии продолжает набирать обороты, что требует от организаций особого внимания к облачной безопасности.

Это включает в себя защиту данных, хранящихся в облаке, обеспечение безопасности API, а также управление доступом и идентификацией в облачной среде. Также важным аспектом является безопасность конфигурации облачных сервисов, поскольку неправильно настроенные облачные ресурсы часто становятся целью атак.

Противодействие внутренним угрозам

Внутренние угрозы — это один из наиболее сложных для обнаружения типов рисков. Они могут включать в себя не только преднамеренные действия сотрудников, но и случайные ошибки, приводящие к утечкам данных или другим проблемам безопасности.

В 2024 году важно будет не только технологически контролировать и мониторить действия сотрудников, но и проводить регулярное обучение персонала, чтобы повысить осведомленность о потенциальных угрозах и методах их предотвращения.

Киберпреступность как услуга

Развитие киберпреступности как услуги *(Cybercrime-as-a-Service)* означает, что даже неопытные злоумышленники могут получить доступ к продвинутым инструментам для осуществления атак.

Это включает в себя всё - от аренды вредоносного ПО до покупки готовых кибератак на черном рынке. В результате барьер для входа в киберпреступность снижается, что может привести к увеличению числа и разнообразия атак. Организациям необходимо быть готовыми к более широкому спектру угроз и иметь комплексные системы защиты.

Вредоносные программы-вымогатели

Вредоносные программы-вымогатели часто воспринимаются как более распространенная и разрушительная угроза информационной безопасности. Данная угроза остается значительной и ожидается сохранение ее важности в следующем году.

Киберпреступники будут использовать более сложные и утонченные методы, в том числе внедрение программ-вымогателей, основанных на искусственном интеллекте. Эти программы будут способны адаптироваться к изменениям в среде безопасности и обходить традиционные меры защиты.Надо подчеркнуть, что тактика двойного вымогательства, при которой злоумышленники сначала крадут конфиденциальные данные, а затем шифруют их, будет дальше развиваться, создавая дополнительное давление на потенциальных жертв и вынуждая их платить выкуп.

Обучение и подготовка кадров

Недостаток квалифицированных специалистов в области кибербезопасности продолжает оставаться проблемой для многих организаций. Ожидается, что спрос на обученные кадры в этой области будет расти.
Организациям необходимо инвестировать в обучение и развитие своих сотрудников, чтобы подготовить их к эффективному реагированию на угрозы информационной безопасности. Это может включать в себя специализированные курсы, воркшопы, участие в симуляциях кибератак и регулярные тренинги по повышению осведомленности в области информационной безопасности.

Кроме того, университеты и образовательные учреждения, возможно, будут расширять и углублять свои программы по информационной безопасности, чтобы удовлетворить растущий спрос на специалистов.

Тенденции в области кибербезопасности на 2024 год показывают, что организациям предстоит столкнуться с рядом новых и усиливающихся угроз. Это требует комплексного подхода, включающего в себя технологические инновации, обучение персонала, соблюдение законодательства и международное сотрудничество. Постоянное обновление знаний и навыков, а также адаптация к изменяющимся условиям будут ключевым фактором успешной защиты от угроз информационной безопасности.

Инциденты в области информационной безопасности, произошедшие в Казахстане за последний год, позволяют нам не только оценить текущую ситуацию, но и выявить области, где необходимо сосредоточить усилия для улучшения безопасности наших цифровых пространств. Уроки, извлеченные из этих событий, являются ценными ресурсами для развития более эффективных стратегий защиты от угроз ИБ в будущем.

Проанализировав последние события, мы видим, что киберпреступники по-прежнему развивают свои методы и тактики, стремясь к новым высотам сложности и коварства, от атак на личные данные до нападений на корпоративные системы. Каждый инцидент становится напоминанием о важности укрепления наших мер безопасности и совершенствования навыков противостояния угрозам ИБ.

Однако вместе с вызовами приходит и понимание, что только совместными усилиями, достойным образованием и внедрением передовых технологий мы сможем наращивать оборонную линию против киберпреступников. Эффективные стратегии информационной безопасности требуют постоянного внимания, обучения и активного взаимодействия сообщества, бизнеса и государства. Только совместные усилия могут сделать наше цифровое будущее более безопасным и устойчивым.

Будем надеяться, что следующий год будет периодом новых достижений и совместных успехов в обеспечении кибербезопасности в Казахстане. Благодарим за внимание к нашему кибердайджесту и ждем вас в следующем издании.

С наилучшими пожеланиями, команда «STS»

Источники и сноски

www.tadviser.ru
Портал выбора технологий и поставщиков.

www.ixbt.com
Российское информационно-аналитическое интернет-издание о компьютерных технологиях.

www.sentinelone.com
Американский стартап в области кибербезопасности, базирующийся в Маунтин-Вью (Mountain View), штат Калифорния (California).

www.anti-malware.ru
Независимый российский информационно-аналитический центр, Интернет-проект, посвящённый вопросам обеспечения информационной безопасности и противодействия вредоносному программному обеспечению.

www.sts.kz
Официальный интернет-ресурс акционерного общества «Государственная техническая служба».

www.cert.gov.kz
Официальный интернет-ресурс Национальной службы реагирования на компьютерные инциденты KZ-CERT.