ОБЗОР СИТУАЦИИ В КИБЕРПРОСТРАНСТВЕ

КИБЕРДАЙДЖЕСТ

2022 ГОД

КИБЕРДАЙДЖЕСТ: СОДЕРЖАНИЕ

В МИРЕ

В КАЗАХСТАНЕ

ВВЕДЕНИЕ

Кибербезопасность всегда была актуальной проблемой для большинства отраслей, но после COVID-19 и последующим за ним переходом на дистанционный режим работы эта проблема стала более острой, поскольку большая часть компаний хранят конфиденциальные и персональные данные пользователей на незащищенных устройствах, что ведет к увеличению роста хакерских атак. Во время пандемии коронавируса поток информации в виртуальном пространстве увеличился, вследствие чего киберпреступники активно нацелились на банковский сектор и сектор здравоохранения, подвергая многих людей и компании риску из-за проблем с ответственностью и конфиденциальностью. Основной причиной большинства вторжений *(кибератак)* является человеческий фактор.

Текущая геополитическая ситуация не только способствует увеличению известных киберугроз, затрагивающих бизнес-сферу, но и влечет другие непредсказуемые риски, которые могут привести к достаточно серьезным последствиям. Все больше организаций наращивают свои вычислительные мощности, добавляют серверы, рабочие станции, сетевые и прочие устройства, а цены на оборудование продолжают расти. В таких условиях начинают сокращаться затраты на кибербезопасность, на приобретение оборудования или продление лицензии на ПО.

Бизнес-сфере стоит обратить внимание на следующие тенденции кибербезопасности, которые, вероятно, получат более широкое распространение в ближайшие годы.

Осведомленность о кибербезопасности

ПОСЛЕДНИЕ ГОДЫ ДОМИНИРУЮЩЕЕ ПОЛОЖЕНИЕ ЗАНИМАЮТ КИБЕРАТАКИ С ПРИМЕНЕНИЕМ ФИШИНГА

Последние годы, по данным ГТС, доминирующее положение занимают кибератаки с применением фишинга, когда злоумышленники, используя неподготовленность сотрудников, с использованием фишинга осуществляют запуск вредоносного программного обеспечения *(для удаленного доступа, вредоносный загрузчик или вирус-шифровальщик и др.)*, крадут учетные данные, которые используются для доступа к корпоративным сетям или базам данных с конфиденциальной или персональной информацией, в том числе к аккаунтам социальных сетей и интернет-банкингу. Отмечается тенденция распространения геотаргетированных фишинговых угроз, когда киберпреступник сосредотачивается на определенной локации, создавая максимально эффективную атаку в зависимости от цели. Например, имитируется какой-то бренд или организация с приобретением доменных имен в зоне .kz или.қаз и т.д., чтобы выглядеть как можно более легитимными.

Потенциально уязвимое облако

После COVID-19 большинство предприятий перешли на облако для хранения конфиденциальных данных. Однако большинство облачных провайдеров не обеспечивают безопасное шифрование, безопасную аутентификацию и ведение журналов аудита в качестве мер безопасности, что создает значительные неудобства для организаций, имеющих дело с особо конфиденциальными или персональными данными.

Атаки на цепочку поставок

Не является секретом для злоумышленников использование крупными организациями сторонних ПО, которые зачастую не являются безопасными. Проникнуть в систему и получить доступ к методам и данным они могут, используя третьи лица или поставщиков. Поэтому организации должны внедрять строгие стандарты целостности кода, которые позволяют работать только авторизованным приложениям для защиты от атак на цепочку поставок.

DDoS-атаки с вымогательством

РАСПРЕДЕЛЕННЫЕ АТАКИ ПО ТИПУ ОТКАЗ ОТ ОБСЛУЖИВАНИЯ ДОСТИГЛИ БЕСПРЕЦЕДЕНТНОГО РАСПРОСТРАНЕНИЯ В 2022 ГОДУ.

Распределенные атаки по типу отказ от обслуживания, направленные на подавление и отключение критически важных сетевых систем организации-жертвы, достигли беспрецедентного распространения в 2022 году. Злоумышленники организовали другую DDoS активность - глобальную кампанию по вымогательству, также известную как «DDoS с выкупом» или RDDoS, когда они угрожают запустить DDoS-атаку, если требование выкупа не будет выполнено к указанному сроку. С ростом количества DDoS-вымогательств увеличиваются риски для неподготовленных организаций.

По мере увеличения числа подключенных к Интернету устройств возрастает и угроза, которую злоумышленники могут использовать для доступа к жизненно важной инфраструктуре организации. Таким образом, предприятия должны подготовиться и спланировать эту тенденцию в области кибербезопасности, которая станет более заметной в ближайшие годы.

МИРОВЫЕ ТРЕНДЫ УГРОЗ И ИНЦИДЕНТОВ ИБ

ИНЦИДЕНТЫ ИБ В МИРЕ

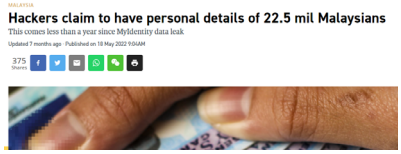
Утечка данных
Data leak


Texas Tech University Health Sciences Center and Baptist Health Report Data Breaches of Over 1.2 Million Records

Posted By HIPAA Journal on Jun 24, 2022

Texas Tech University Health Sciences Center has confirmed that the protected health inform
1,290,104 patients was compromised in a data breach at its electronic medical record vendor

источник: https://www.hipaajournal.com/almost-1-3-million-patients-of-texas-tech-university-health-sciences-center-affected-by-eye-care-leaders-data-breach/)


MALAYSIA

Hackers claim to have personal details of 22.5 mil Malaysians

This comes less than a year since MyIdentity data leak

Updated 7 months ago · Published on 18 May 2022 9:04AM

375 Shares

источник: https://www.thevibes.com/articles/news/61117/hacker-group-claims-to-have-personal-details-of-22.5-mil-malaysians

Согласно отчету Positive Technologies, наиболее похищаемыми данными организаций стали персональные данные (36%) и сведения, содержащие коммерческую тайну (11%). У частных лиц чаще похищали учетные и персональные данные, на которые пришлись 41% и 24% соответственно. Подобные утечки подвергают огромное количество людей риску подделки их цифровой личности и совершения несанкционированных действий от их имени. Предлагается рассмотреть краткую сводку кибератак на инфраструктуры международных организаций.

Громкими утечками конфиденциальных данных можно назвать **атаку на сеть медицинских учреждений Baptist Health,** которая затронула более миллиона человек и скомпрометировала их персональные данные и медицинскую информацию, а также **взлом платформы Национального регистрационного департамента Малайзии,** в результате которого были похищены и выставлены на продажу на одном из теневых форумов уникальные идентификаторы, фотографии и номера телефонов более 22 миллионов граждан страны.

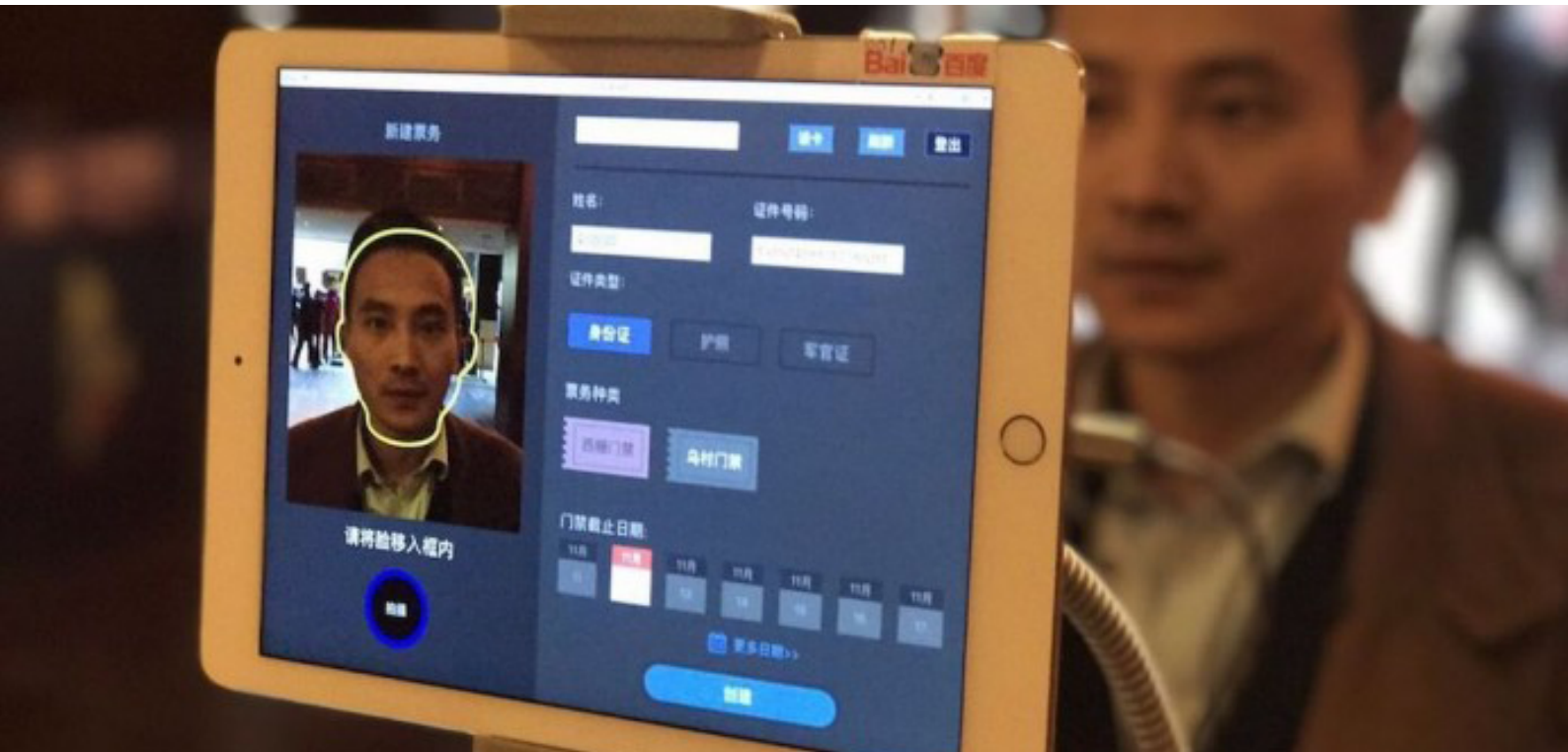
Злоумышленники похитили данные 1 млн пользователей Facebook, распространяя вредоносные приложения, сообщил директор Meta по борьбе с киберугрозами Дэвид Агранович. Всего злоумышленники распространили в магазинах приложений Google и Apple более 400 мобильных приложений. Эти программы выполняли функции фоторедакторов и других сервисов и провоцировали вводить данные от учетных записей Facebook. После загрузки программы пользователю предлагали настроить учетную запись, для чего требовалось войти в аккаунт. Введенные данные программы пересылали злоумышленникам. Кроме фоторедакторов (около 40%) среди вредоносных программ встречались игры, утилиты для бизнеса и другие. В магазине приложений для iOS таких приложений было 47, а в Google Play для платформы Android — 355. Обе компании сообщили, что все вредоносные приложения уже удалили.
Одна из последних крупных утечек пользовательских данных на Facebook произошла в апреле 2021 года. Тогда в Сеть утекли данные примерно 500 млн человек из 106 стран.

В середине 2021 года **компании Apple Inc. и Meta Platforms Inc. подверглись атаке хакеров,** которые, выдавая себя за сотрудников правоохранительных органов, скомпрометировали персональные данные пользователей. Среди такой информации оказались адреса, номера телефонов и IP-адреса пользователей. Указанные персональные данные в основном передаются по экстренным запросам органов без постановления суда, чем и воспользовались злоумышленники. Конфиденциальная информация, полученная хакерами с помощью поддельных юридических запросов, может применяться в разнообразных схемах финансового мошенничества. Хакеры могли использовать информацию о жертвах, чтобы

обойти защиту их учетных записей в популярных приложениях, мессенджерах или электронных почтах. Специалистами высказано мнение, что мошеннические юридические запросы информации о пользователях являются частью многомесячной кампании, начавшейся в январе 2021 года и направленной против многих технологических компаний. Вероятно, поддельные юридические запросы отправляются через взломанные домены электронной почты, принадлежащие правоохранительным органам в нескольких странах, и зачастую содержат поддельные подписи настоящих или вымышленных сотрудников.
Представители Apple и Meta регулярно публикуют сведения о своей деятельности по обратной связи. Так, с июля по декабрь 2020 года Apple получила 1162 запроса на экстренную помощь из 29 стран и предоставила данные в ответ на 93% этих запросов. Meta сообщает, что с января по июнь 2021 года получила 21 700 экстренных запросов по всему миру и частично предоставила персональные данные в ответ на 77% запросов.

Утечка конфиденциальной информации из системы распознавания лиц в Китае

Разработчики ПО для распознавания лиц не учли защиту своей базы с конфиденциальной информацией, поэтому в течение нескольких месяцев **в открытом доступе находилась огромная база с конфиденциальной информацией** миллионов граждан Китая. Объем скомпрометированной базы постоянно пополнялся и на пике наблюдения она содержала более 800 млн записей. Таким образом, это одна из крупнейших утечек в 2022 году.
Более масштабный инцидент произошел в июне 2022 года, когда **из полиции Шанхая утекли 1 млрд записей персональных данных.** Скомпрометированные данные принадлежали китайской компании Xinai Electronics, которая разрабатывает системы доступа для людей и автотранспорта. В частности, решения на базе их ПО используются на рабочих местах, в школах, на стройплощадках и в паркингах. Благодаря развертыванию сети камер, Xinai накопила многие миллионы биометрических данных и фотографий номерных знаков автомобилей.
Незащищенную базу на облачном сервере Alibaba обнаружил исследователь кибербезопасности Анураг Сен (Anurag Sen).



Утекли персональные данные у новой авиакомпании в Индии

Недавно созданная авиакомпания Akasa Air начала свою деятельность с утечки информации – были скомпрометированы персональные данные пассажиров, которые воздушный перевозчик потерял из-за сбоя в системе регистрации.
Исследователь кибербезопасности Ashutosh Barot обнаружил утечку конфиденциальной информации Akasa Air в первый день работы этой компании. Открытая конфиденциальная информация включала ФИО, электронные адреса, половую принадлежность, а также номера телефонов пассажиров, которые регистрировались в системе Akasa Air. Barot выявил утечку информацию путем HTTP-запроса на сайте авиакомпании.
Представители Akasa Air признали, что инцидент информационной безопасности поставил под угрозу более 34 тыс. уникальных записей персональных данных пассажиров. Авиакомпания Akasa Air уже уведомила об инциденте индийское Национальное агентство по кибербезопасности (CERT-In).

Утечка конфиденциальной информации 2,5 млн студентов

В результате кибератаки на финансовую организацию Nelnet была скомпрометирована конфиденциальная информация в отношении 2,5 млн. студентов американских вузов. Компания Nelnet является технологическим партнером ряда кредитных организаций, включая Edfinancial и Oklahoma Student Loan Authority (OSLA), в создании и поддержке личных кабинетов студентов, являющихся заемщиками ссуды на обучение. Конфиденциальная информация учетных записей, а именно контактная информация и номера социального страхования были украдены хакерами.
В июле Nelnet уведомили своих клиентов Edfinancial и OSLA об обнаруженной уязвимости, спровоцировавшей кибератаку, и сообщили, что предприняли меры по устранению проблемы и обеспечению информационной безопасности. Расследование инцидента показало, что хакеры имели доступ к персональным данным студентов с июня по июль 2022 г. Согласно уведомлению, направленному в прокуратуру, в результате утечки конфиденциальной информации пострадали 2 501 324 человека, которым предоставили услуги кредитного мониторинга на 24 месяца.

Panasonic вновь потерял конфиденциальную информацию

Panasonic

Японский ИТ-гигант Panasonic заявил, что подразделение в Канаде потеряло конфиденциальную информацию в результате хакерской атаки. Это третья утечка из Panasonic менее чем за полгода.
Компания Panasonic в феврале 2022 года подверглась хакерской атаке, в результате которой были скомпрометированы некоторые системы и процессы. Сотрудник Panasonic Airi Minobe подчеркнул, что были выполнены все необходимые действия после атаки. Оценив масштабы инцидента, компания нашла способы сдержать вредоносное ПО, восстановила серверы и наладила коммуникации с пострадавшими клиентами и правоохранительными органами.
По данным команды кибериссследователей VX-Underground, атака на канадский филиал Panasonis была организована хакерами из группировки Conti, распространяющими вредоносное ПО, в том числе по модели RaaS (сдача ресурсов для

распространения вирусов в аренду). По данным Mitsui Bussan Secure Direction, в распоряжении вымогателей оказались 6100 файлов объемом 2,87 гигабайта. Похищенные файлы содержали информацию о персонале, бюджете и данные бухгалтерского учета.
В ноябре 2021 г. компания Panasonis призналась в том, что в их сеть проникли неизвестные и получили ряд данных с файлового хранилища. Позже в компании уточнили, что хакеры украли персональные данные соискателей и стажеров. Кроме того, в декабре 2021 г. атаке с использованием вируса-вымогателя подверглось подразделение Panasonic в Индии. В результате в руки хакеров попали 4 ГБ данных, включая финансовую информацию и адреса электронной почты.

Программы-вымогатели

Программы-вымогатели Cl0p

Британская компания South Staffordshire Water, которая поставляет 330 млн литров пригодной для питья воды 1,6 млн клиентам в сутки, 16 августа 2022 года выпустила сообщение, в котором подтвердила нарушения, возникшие в работе ИТ-систем вследствие кибератаки. Распространители вымогателя взяли на себя ответственность за данную атаку. Злоумышленники не нарушили поставки воды населению, но явно дали понять о своем присутствии внутри сети. South Staffordshire Plc, материнская компания коммунальных служб Cambridge Water и South Staffordshire Water заверила своих клиентов, что их водоснабжение после очевидной атаки программы- вымогателя Clop (также известной как Cl0p) находится в безопасности.

Округ Берналилло, штат Нью-Мексико – как инциденты в киберпространстве влияют на окружающий нас мир?

5 января 2022 года крупнейший округ в Нью-Мексико стал жертвой атаки программы-вымогателя, в результате чего работоспособность инфраструктуры нескольких окружных департаментов и правительственных учреждений была парализована. Официальные лица округа уверяли общественность, что не производили оплату хакерам.
Помимо серьезного беспокойства граждан, которое сопровождает отключение любого государственного ведомства, эта атака программы-вымогателя привлекла особое внимание, поскольку в результате была заблокирована работоспособность инфраструктуры исправительного учреждения округа: вывела из строя камеры видеонаблюдения и автоматические двери, заключенных пришлось держать в своих камерах. Выход из строя электронных замков на дверях камер вынудило учреждение строго ограничить передвижение заключенных, что явилось потенциальным нарушением 25-летнего мирового соглашения об условиях содержания заключенных.
Округу пришлось подать экстренное уведомление в федеральный суд из-за неспособности выполнить соглашение из-за атаки вредоносного ПО.

Toyota – кибератака, принесшая многомилионные потери автогиганту

В период с февраля по март 2022 года кибератакам были подвержены три поставщика Toyota - Kojima Industries, Denso и Bridgestone.
Когда компания Kojima Industries подверглась кибератаке, гиганту пришлось остановить работу 14 своих японских заводов. По некоторым сведениям, указанный взлом привел к колоссальному 5-процентному падению ежемесячных производственных мощностей компании.
Denso и Bridgestone стали жертвами атак программ-вымогателей в течение 11 дней. Дочерняя компания Bridgestone подверглась атаке программ-вымогателей, в результате чего были отключены компьютерные сети и производственные мощности в Средней и Северной Америке. Ответственность за эту атаку взял на себя Lockbit. В случае с Denso группа компаний в Германии предположительно была скомпрометирована группой вымогателей Pandora.
Независимо от того, насколько защищена ваша организация, решительный злоумышленник может и найдет способ взломать ее. Даже предприятия с ресурсами Toyota становятся жертвами масштабных кибератак.

DDoS-атаки

Сервера госслужб

13 сентября 2022 г. подвергся DDoS-атаке официальный сайт ОДКБ odkb-csto.org. Была нарушена доступность ресурса, зафиксированы несанкционированные попытки внесения изменений в некоторые информационные сообщения, в течение суток доступ к ресурсу был невозможен. Позже работоспособность интернет-ресурса была частично восстановлена, однако по-прежнему ведутся мероприятия по локализации несанкционированного вмешательства и восстановлению поврежденных или утраченных данных.

Google отразила сильнейшую DDoS-атаку в истории

Компания Google в июне 2022 года заблокировала крупнейшую в истории атаку типа «отказ в обслуживании» (DDoS) по протоколу HTTPS. Ее мощность на пике достигала 46 миллионов запросов в секунду (RPS). Жертвой атаки стал неназванный клиент Google Cloud Armor (GCA). GCA - киберзащитный сервис и балансировщик нагрузки веб-приложений. Инцидент произошел 1 июня 2022 года и продолжался в течение 69 минут.
Атака началась с нагрузки в 10 тысяч RPS, уже через восемь минут мощность возросла до 100 тысяч RPS, а еще через две минуты — до 46 млн RPS. Вредоносный трафик исходил от 5256 IP-адресов, зарегистрированных в 132 странах. Почти треть всех запросов пришлась на Бразилию, Индию, Россию и Индонезию. В Google назвали источником DDoS-атаки ботнет Mēris. В сентябре прошлого года эта сеть, состоящая из нескольких сотен тысяч зараженных устройств, атаковала «Яндекс». Мощность атаки составила 20 миллионов RPS, что на тот момент делало ее самой крупной из известных за всю историю интернета.

Несанкционированный доступ и модификация содержания

Гостиничный бизнес

В начале сентября 2022 года IT-системы крупной гостиничной сети InterContinental Hotels Group, управляющей 17 гостиничными брендами по всему миру, были взломаны, что привело к нарушению работы систем онлайн-бронирования и других сервисов корпорации. InterContinental Hotels Group (IHG), штаб-квартира которой находится в Англии, а офисы в Атланте, Сингапуре и Шанхае, сообщила в заявлении, что некоторые из ее технологических систем подверглись несанкционированным действиям. Далее компания сообщила, что ее деятельность была нарушена с 5 сентября 2022 года, в результате чего люди испытывали трудности, особенно с бронированием номеров через интернет.

Европейские нефтяные портовые терминалы пострадали от кибератаки

Прокуратура Антверпена (Бельгия) сообщила о начале расследования масштабной кибератаки против портовой инфраструктуры. Крупные нефтеналивные терминалы в некоторых крупнейших портах Западной Европы стали жертвами кибератаки 28 января. Хакеры взломали операционные системы терминалов Evos во фламандских портах Антверпен и Гент, а также голландские порты Тернезен и Амстердам. В результате значительная часть компьютерных мощностей компании вышла из строя, фактически блокировав работу принадлежащих ей инфраструктурных объектов.
Кибератаки привели к задержкам при погрузке и разгрузке нефтеналивных танкеров. В результате судам приходится дольше ждать, прежде чем их можно будет обработать. Любые длительные задержки влияют на цены.

Недоступность интернет-ресурсов

Атака на воздушные гавани

В США 10 октября 2022 года недоступными оказались сайты 14 крупнейших аэропортов страны. Ответственность за инцидент взяли российские хакеры из группировки Killnet, ранее называвшие эти объекты в качестве своих целей. Первые атаки зафиксировали около 3:00 в аэропорту Ла-Гуардия в Нью-Йорке. Позднее специалисты отмечали сбои в работе сайтов международного аэропорта Лос-Анджелеса и международного аэропорта О'Хара в Чикаго.
Атаки нарушили доступ к сайтам, информирующим о загруженности и времени ожидания в аэропортах. Однако действия хакеров не затронули управление воздушным движением, транспортную безопасность и линии связи с самолетами.

ОБЗОР МЕЖДУНАРОДНЫХ ПРОГНОЗОВ ПО КИБЕРБЕЗОПАСНОСТИ НА 2023 ГОД

Представители Лаборатории Касперского 8 декабря 2022 года представили свой прогноз **по трендам в области угроз кибербезопасности** для корпораций и крупных организаций в 2023 году.

Продолжится рост числа утечек персональных данных

Эта тенденция получит новый виток, когда злоумышленники будут не просто «сливать» базы, но и совмещать информацию из различных источников. В результате они смогут получать подробное «досье» на человека и затем реализовывать более продвинутые, таргетированные схемы социальной инженерии и кибершпионажа в атаках на бизнес.

Покупка готовых доступов

В 2023 году злоумышленники будут чаще обращаться к ресурсам даркнета за покупкой доступов к уже скомпрометированным сетям разных организаций. Всё чаще атаки начинаются с использования полученной ранее информации об учётных записях пользователей, опубликованных на теневых ресурсах.
Этот тренд опасен тем, что этап компрометации данных может оставаться незамеченным. Только получив ощутимый ущерб (например, столкнувшись с перебоями в работе сервиса или шифрованием данных), компания-жертва узнает о совершённой атаке.

---

22 ноября 2022 года компания **Atakama,** специализирующаяся на разработке решений в сфере киберзащиты, обнародовала **прогноз в области информационной безопасности** на 2023 год. Авторы исследования выделяют несколько ключевых тенденций.

Интернет вещей Internet of Things (IoT) сливается с «теневыми ИТ», создавая угрозу безопасности

В 2023 году к интернету будут подключены приблизительно 43 млрд. самых разных устройств, что предоставит злоумышленникам широчайший выбор для совершения противоправных действий. Производители IoT-оборудования отдают предпочтение удобству и потребительской привлекательности, а не средствам обеспечения безопасности. Зачастую такие устройства внедряются в инфраструктуру компании с учётными данными по умолчанию. Более того, интернет вещей совмещается с теневыми ИТ-системами, создавая угрозу несанкционированного проникновения даже в надёжно защищённые сети.

Рост интенсивности изощрённых атак программ-вымогателей с целью кражи данных

В 2023 ГОДУ ПРОДОЛЖИТ УВЕЛИЧИВАТЬСЯ КОЛИЧЕСТВО АТАК С ПРИМЕНЕНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

В 2023 году продолжит увеличиваться количество атак с применением программ-вымогателей. У злоумышленников появилось больше способов монетизировать конфиденциальные данные жертв. Помимо шифрования информации с целью получения выкупа киберпреступники могут выставлять похищенные файлы на продажу в даркнете или же публиковать их в открытом доступе. В такой ситуации организациям придётся выйти за рамки традиционных методов защиты данных и перейти к внедрению новых методов: это может быть, например, многофакторное шифрование, которое сделает файлы бесполезными для злоумышленников.

DevSecOps выйдет на новый уровень.

Защита сред разработки станет одним из наиболее важных направлений для достижения эффективной безопасности организаций в 2023 году. Включение всего нескольких строк вредоносного кода на этапе создания приложения потенциально может открыть для злоумышленников тысячи мишеней в цепочках поставок партнёров и клиентов. Поэтому усиленные методы DevSecOps *(обеспечение безопасности на всех этапах разработки приложений)* в соответствии с архитектурой нулевого доверия и передовыми решениями для шифрования данных станут более распространёнными. Организации осознают, что такой подход является критической необходимостью для бизнеса.

Gartner назвал 5 главных трендов в сфере защиты конфиденциальности данных на ближайшие пару лет

Gartner®

В конце мая 2022 года аналитики Gartner опубликовали исследование, в котором перечислили, по их мнению, 5 главных трендов в сфере защиты конфиденциальности данных на ближайшие пару лет. Имея в виду эти тенденции, бизнес может минимизировать проблемы защиты персональных данных и выполнения нормативных требований, считают эксперты.
С учетом распространения норм регулирования конфиденциальности на десятки юрисдикций, вплоть до 2024 года многие организации увидят необходимость начать реализацию своих программ по защите конфиденциальности. Фактически, по прогнозам Gartner, средний годовой бюджет крупных организаций на обеспечение конфиденциальности данных к 2024 году превысит $2,5 млн. Gartner выделила пять тенденций в области защиты данных, которые способствуют развитию практики конфиденциальности.

Локализация данных

Страны стремятся установить контроль над данными при помощи их локализации. Такой контроль является либо прямым требованием, либо побочным продуктом многих новых законов о конфиденциальности.
Компании все чаще сталкиваются с различными нормативно-правовыми условиями, когда в разных регионах требуются различные стратегии локализации. В результате планирование локализации данных станет одним из главных приоритетов при разработке и приобретении облачных услуг.

Методы вычислений, повышающие конфиденциальность

Обработка данных в ненадежных средах, таких как публичное облако и многосторонний обмен данными и аналитика, приобрели основополагающее значение для большинства организаций.
Растущая сложность аналитических движков и архитектур требует от поставщиков облачных услуг внедрения возможностей обеспечения конфиденциальности на уровне разработки. По прогнозам Gartner, к 2025 году 60% крупных организаций будут использовать хотя бы один метод вычислений с повышенной конфиденциальностью (PEC) в аналитике, бизнес-аналитике и/или облачных вычислениях.

Регулирование искусственного интеллекта (ИИ)

ИССЛЕДОВАНИЕ GARTNER ПОКАЗАЛО, ЧТО 40% ОРГАНИЗАЦИЙ НАРУШАЛИ ПРИВАТНОСТЬ С ПОМОЩЬЮ ИИ И ЧТО ЧЕТВЕРТЬ ЭТИХ НАРУШЕНИЙ БЫЛИ ЗЛОНАМЕРЕННЫМИ

Исследование Gartner показало, что 40% организаций нарушали приватность с помощью ИИ и что четверть этих нарушений были злонамеренными. Независимо от того, обрабатывают ли организации персональные данные, риски для конфиденциальности и потенциального неправомерного использования персональных данных очевидны.
Большая часть ИИ, используемого сегодня в организациях, встроена в большие, комплексные решения, а надзор для оценки влияния на конфиденциальность практически отсутствует. Эти встроенные возможности ИИ используются для отслеживания поведения сотрудников, оценки настроения потребителей и создания «умных» продуктов. Более того, данные, которые сегодня поступают в эти обучающиеся модели, будут оказывать влияние на принимаемые решения спустя годы, - говорит вице-президент Gartner Надер Хенейн.

Централизованный пользовательский интерфейс конфиденциальности

Растущий потребительский спрос на права пользователей и возросшие ожидания в отношении прозрачности приведут к необходимости создания централизованного пользовательского интерфейса конфиденциальности (UX). Дальновидные организации понимают преимущество объединения всех аспектов пользовательского интерфейса конфиденциальности, таких как уведомления, файлы cookie, управление согласованиями и обработка запросов о правах субъектов (SRR), на одном портале самообслуживания. Такой подход обеспечивает удобство для ключевых участников, клиентов и сотрудников, а также значительную экономию времени и средств.

Дистанционный контроль становится «гибридным всем»

Поскольку во многих организациях модели взаимодействия становятся более гибридными, размывая грань между работой и личной жизнью, растет возможность отслеживания, мониторинга и других действий по обработке персональных данных, а риск нарушения конфиденциальности становится первостепенным. Учитывая последствия для конфиденциальности, связанные с гибридным подходом к взаимодействию, производительность и удовлетворенность балансом между работой и личной жизнью также возросли в ряде сфер деятельности и профессий.

АНАЛИЗ ОСНОВНЫХ ВЕКТОРОВ АТАК НА РК

Базу данных «Казпочты» продают в Сети за 25 тысяч долларов

13 июня 2022 года представители Центра анализа и расследования кибератак (ЦАРКА) сообщили, что на одном из хакерских форумов выставлен на продажу доступ к серверу бэкапа баз данных АО «Казпочта».
В объявлении было указано, что база данных представляет собой 44 таблицы общим размером 110 ГБ и содержит около 12 млн записей.
В базе данных содержалась следующая информация:

- данные о почтовых отправлениях;
- автострахование;
- запросы на кредиты;
- депозиты;
- денежные переводы;
- открытие счетов и карт;
- информация о сотрудниках *(должность, ФИО, адрес, номер телефона);*
- основные персональные данные: полный адрес, номер телефона, ФИО, дата рождения, паспортные данные, почта, полис автострахования, частичные номера банковских карт и многое другое.

В АО «Казпочта» заявили, что утечки с их серверов не происходило. Физическое лицо, разместившее объявление на хакерском форуме о доступе к серверу бэкапа баз данных «Казпочты», неоднократно обращалось в компанию с целью шантажа, предлагая выкупить за несколько тысяч долларов материалы годичной давности, которые были получены им со стороннего сервера. Информация о шантаже была передана в правоохранительные органы для привлечения к ответственности физического лица.

31 канал был атакован шифровальщиком

Сотрудниками «31 канала» были обнаружены зашифрованные файлы с подозрительными расширениями на файловом сервере компании. Для нейтрализации угроз технические администраторы «31 канала» отключили сетевые интерфейсы на зашифрованных серверах. Затем системный администратор заметил следы вредоносного программного обеспечения, запущенного под локальным администратором с помощью программ ProcessHackek, UBitUnlocker. Также с этого сервера были замечены подключения по протоколу RDP к другим серверам со взломом аккаунтов локальных администраторов. В списке зашифрованных серверов были замечены серверы, связанные с программой 1С, файловым сервером бухгалтерии, Wi-Fi, сервером печати и др. Злоумышленникам удалось вручную удалить установленное антивирусное ПО на всех серверах. Проведенное сканирование зашифрованных серверов установило, что зараженные серверы, находящиеся в одной виртуальной локальной компьютерной сети, имели уязвимость, связанную с авторизацией. Резервное копирование данных не осуществлялось своевременно.

Казахстанские пользователи Telegram пожаловались на массовые взломы аккаунтов

Казахстанские пользователи Telegram пожаловались на спам-рассылки, с помощью которых хакеры могли получить доступ к конфиденциальной информации. Приходило сообщение с рекламой некого чат-бота, при переходе на который пользователь получал сообщение с просьбой пройти верификацию *(проверку на достоверность внесённых данных)*. Далее на мобильный телефон пользователя поступает SMS с кодом, который необходимо ввести. После осуществления предлагаемого действия все контакты и группы пользователя получают такие же сообщения с рекламой этого чат-бота.
Особенно уязвимыми оказались аккаунты пользователей, которые не включили двухфакторную аутентификацию входа в учётную запись *(система доступа, основанная на двух «ключах»: SMS с кодом и логин с паролем)*.

Хакеры взломали интернет-ресурс православной митрополии Казахстана

В результате проведенных злоумышленниками кибератак был взломан интернет-ресурс Митрополичьего округа. Митрополит Астанайский и Казахстанский Александр обратился в ГТС с просьбой установить источник атаки и обеспечить безопасность ресурса. Доступность ресурса удалось восстановить, однако длительная остановка его работоспособности вызвала беспокойство у аудитории, которая насчитывает тысячи постоянных пользователей. За 12 лет на ресурсе накопилось большое количество контента, представляющего значительную архивную ценность. По сведениям хостинг-провайдера система управлении контентом интернет-ресурса митрополии содержала уязвимости, которыми воспользовались хакеры. Вероятность повторных действий со стороны хакеров оценивают как высокую.

ЗАКЛЮЧЕНИЕ

ПОЛЬЗОВАТЕЛИ ПО-ПРЕЖНЕМУ ОСТАЮТСЯ ОСНОВНЫМ ИСТОЧНИКОМ РИСКОВ ИБ В ЛЮБОЙ ОРГАНИЗАЦИИ

Пользователи по-прежнему остаются основным источником рисков ИБ в любой организации. Независимо от информационной подготовки сотрудники могут предоставлять злоумышленникам начальный вектор атаки за счёт социальной инженерии, фишинга и других мошеннических схем. По оценкам экспертов, человеческий фактор был «ключевой движущей силой» в 82% утечек данных. Риски ИБ со стороны работников партнёрских организаций и сторонних поставщиков потребуют от организаций постоянной бдительности и усиленного внедрения стратегии нулевого доверия.
В связи с ростом интенсивности кибератак и необходимостью поддержания защиты на должном уровне для руководителей по информационной безопасности важно регулярно обновлять свои знания, поскольку происходит постоянное развитие не только угроз, но и защитных решений. Ответственные лица, которым доверена безопасность и конфиденциальность данных, должны осуществлять деятельность в соответствии с установленными требованиями.

СИТУАЦИЯ В РК

Обеспечение безопасности киберпространства и защита информационно-коммуникационной инфраструктуры - важнейшая задача государства в современном цифровом мире. Именно поэтому информационная безопасность является неотъемлемой частью национальной безопасности.
По поручению Первого Президента Республики Казахстан с 2017 года в стране начата реализация Концепции кибербезопасности «Киберщит Казахстана».
В данном кибердайджесте приведена информация **о тенденциях и угрозах информационной безопасности** за текущий год, прогнозы на следующие годы, а также отражена информация о проделанной ГТС работе* за 2022 год.

ТОП-5 наиболее часто фиксируемого вредоносного программного обеспечения (ВПО) в государственных органах РК*

682 **Not-a-virus:HEUR:AdWare.Script**
– это вердикт, который назначается антивирусным ПО, чтобы указать, что оно обнаружило потенциально нежелательное поведение в файле или программе. «HEUR» в вердикте означает «эвристический анализ», то есть антивирусное программное обеспечение использовало набор правил или эвристик для выявления потенциально нежелательного поведения. Часть вердикта «AdWare.Script» указывает, что оно связано с рекламным ПО, которое представляет собой тип программного обеспечения, отображающего рекламу на компьютере или мобильном устройстве. Рекламное ПО часто связано с другим программным обеспечением и его бывает трудно удалить после его установки.

486 **HEUR:Trojan.WinLNK.Starter.gen**
– троян, имеющий расширение LNK *(ярлык)*, который ссылается на вредоносный файл. При запуске вместе с вредоносным ПО может параллельно запуститься и легитимный файл *(под который мимикрирует ярлык)*.

422 **Worm.NSIS.BitMin.d**
– тип вредоносного ПО, который распространяется по сети. Это позволяет ему заражать большое количество хостов, используя ошибки конфигурации сети *(например, чтобы скопировать себя на полностью доступный диск)*. Также он может заражать компьютеры, используя бреши в защите операционной системы и приложений. NSIS *(Nullsoft Scriptable Install System)* – система установочных программ Windows, созданная компанией Nullsoft. BitMin, CoinMiner, NeksMiner - тип вредоносного ПО, которое использует ресурсы целевой рабочей станции для добычи криптовалюты.

Судя по наибольшему количеству фиксируемых вердиктов на оборудовании в сети распространены черви, которые имитируют рабочие документы.

* - количество уникальных инцидентов в ГО РК.

323 **HEUR:Trojan.Win32.Generic**
– тип ВПО, который относится к семейству троянов. Обычно под этим названием имеется в виду угроза, тип которой пока еще точно не определен.

322 **HEUR:Worm.Win32.FakeDoc.gen**
– исполняемый файл, классифицирующийся как червь, мимикрирует под Word-файл (путем установки значка Microsoft Word, использования двойного расширения и т.д.). Для скрытия запуска вредоносной активности он может параллельно запустить легитимный документ.

ШИФРОВАЛЬЩИКИ

ШИФРОВАЛЬЩИК RANSOMEWARE ПРОГРАММА-ВЫМОГАТЕЛЬ

вредоносное программное обеспечение, цель которого шифрование данных жертвы с последующим получением выкупа за дешифрование.

Шифровальщиками (Ransomware) или как их называют иначе программами-вымогателями принято называть вредоносное программное обеспечение, цель которого шифрование данных жертвы с последующим получением выкупа за дешифрование.
ГТС был отработан инцидент ИБ, связанный с заражением рабочих станций вирусом-шифровальщиком в Национальном институте интеллектуальной собственности МЮ РК. Были зашифрованы данные 34 рабочих станций шифровальщиком семейства «Loki». Изучение артефактов зараженных рабочих станций выявило скомпрометированный узел. На рабочих станциях организации были установлены СЗИ от компании Forti.

Locki Locker – может распространяться путём взлома через незащищенную конфигурацию RDP с использованием email-спама и вредоносных вложений, обманных загрузок, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых загрузчиков. Вирус – шифровальщик выключает множество процессов и сервисов, которые могут помешать шифрованию файлов, отключает Защитник Windows, очищает Корзину и выполняет другие деструктивные действия.
Loki Locker шифрует данные пользователей с помощью комбинации алгоритмов AES-256 (режим GCM) и RSA-2048, а затем требует выкуп в биткойнах.

Файлы, связанные с вирусом-шифровальщиком:
- info.hta, info.Loki - название файла с требованием выкупа в разных вариантах.
- Restore-My-Files.txt - название файла с требованием выкупа.
- Decrypt-info.txt - название файла с требованием выкупа.
- svchost.exe - название вредоносного файла.
- Cpriv.Loki - специальный файл, который нельзя удалять.

Используемые инструменты злоумышленника:
PasswordFox – это небольшая утилита, которая позволяет просматривать логины и пароли, хранящиеся в браузере Mozilla Firefox. По умолчанию PasswordFox отображает пароли в текущем аккаунте.
Advanced IP-Scanner – используется для сканирования сетей. Он находит все доступные устройства в сети, предоставляет доступ к общим папкам и даже может выключить компьютер удаленно.
SniffPass – это небольшая бесплатная программа, которая позволяет отслеживать трафик в беспроводной сети, благодаря которому злоумышленник узнал пароли и ключи, которые были использованы в сети Национального института интеллектуальной собственности МЮ РК.

WirelessKeyView – это альтернатива технической поддержке и самостоятельному восстановлению пароля от WiFi сети.
Mimikatz – инструмент, реализующий функционал Windows Credentials Editor и позволяющий извлечь аутентификационные данные в системе пользователя в открытом виде. Mimikatz – перехват паролей открытых сессий в Windows.
Действия злоумышленника после проникновения в сеть Национального института интеллектуальной собственности МЮ РК были нацелены на кражу данных и вымогательство денежных средств. Предположительно, злоумышленник проник посредством протокола RDP и фишингового письма.

Ботнет

– это сеть компьютеров, удаленно управляемая злоумышленниками.

БОТНЕТЫ

ВСЕГО ЗА 2022 ГОД 59 326 337 *событий*

БОТНЕТ
AAEH
25 778 076 *событий*

БОТНЕТ
njRAT
15 748 429 *событий*

БОТНЕТ
Andromeda
1 469 843 *событий*

БОТНЕТ
Torpig
882 989 *событий*

БОТНЕТ
Formbook
580 302 *событий*

Ботнет AAEH - полиморфный загрузчик с более чем 2 миллионами уникальных образцов

Самым активным в ГО стал ботнет AAEH. После установки он трансформируется каждые несколько часов и быстро распространяется по сетям, съемным дискам (USB / CD / DVD) и через файлы архивов ZIP и RAR. Система, зараженная AAEH, может использоваться для распространения вредоносного ПО, сбора учетных данных пользователей для онлайн-сервисов, включая банковские услуги и вымогательство денег у пользователей путем шифрования файлов. AAEH использовался для загрузки других семейств вредоносного ПО, таких как Zeus, Cryptolocker, ZeroAccess и Cutwail.

njRAT использовался в шпионских кампаниях

Также в число самых распространенных вредоносных программ попал Ботнет njRAT. Троян удаленного доступа njRAT, способный перехватывать управление компьютером жертвы. Согласно мировым отчетам, njRAT использовался в нескольких шпионских кампаниях, проведенных злоумышленниками из разных

стран и регионов. njRAT имеет возможность регистрировать нажатия клавиш, получать доступ к камере жертвы, красть учетные данные, хранящиеся в браузерах, скачивать файлы, просматривать рабочий стол жертвы, выполнять манипуляции с процессами, файлами и реестром, а также позволяет злоумышленнику удалять данные.

Andromeda похищала учетные данные

Третьим по распространению в ГО стал ботнет Andromeda, который впервые был замечен еще в 2011 году и использовался для кражи учетных данных, а также для загрузки и выполнения в зараженных системах другого вредоносного ПО. Согласно имеющимся данным ботнет замечен в распространении более 80 различных семейств вредоносного ПО.

Ботнет имеет возможность собирать данные с компьютера с шагом в 20 минут

Torpig - он же Sinowal, он же Mebroot - доказал, что даже авторитетные бизнес-сайты могут быть скомпрометированы и направлять трафик на вредоносные сайты загрузки. Впервые обнаруженный в конце 2007 года и получивший широкое признание в марте 2008 года, Torpig нацелен на финансовую информацию пользователей, такую как учетные данные банковского счета и кредитной карты. Torpig получил псевдоним «Mebroot» как руткит, заражающий основную загрузочную запись (MBR), которая загружается до загрузки операционной системы компьютера и, таким образом, более трудна для сканирования системами безопасности. Пользователи подхватывали Mebroot на веб-сайтах, скомпрометированных с помощью Javascript, которые приводили их к централизованным серверам загрузки, которые затем заражали устройства ботнетом. Ботнет дал создателям Mebroot контроль над зараженным компьютером и возможность собирать с него данные с шагом в 20 минут.

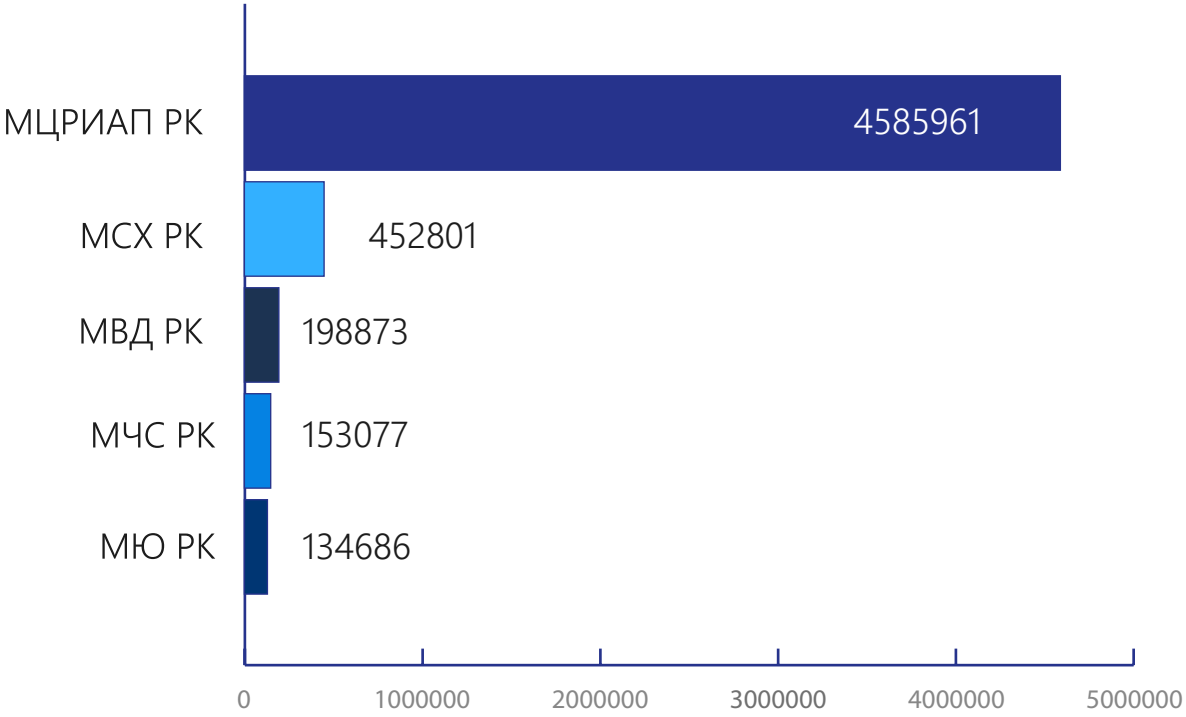
FormBook основан на предоставлении доступа к вредоносным программам для их доставки к цели

Подписчики FormBook покупают средства для развертывания вредоносного ПО, например, встраивают его во вредоносный документ, содержащийся в фишинговом электронном письме. Поскольку само вредоносное ПО не связано с механизмом доставки, FormBook использует различные методы заражения, наиболее распространенными из которых являются фишинговые электронные письма.

После запуска в зараженной системе вредоносная программа FormBook распаковывает свою вредоносную функциональность и внедряет свой код в различные процессы. Этот вредоносный код использует различные перехватчики для получения доступа к нажатиям клавиш, снимкам экрана и другим функциям. Вредоносная программа также может получать от своего оператора команды на кражу информации из браузеров или загрузку и выполнение других вредоносных программ.

FORMBOOK ИСПОЛЬЗУЕТ РАЗЛИЧНЫЕ МЕТОДЫ ЗАРАЖЕНИЯ - ФИШИНГОВЫЕ ЭЛЕКТРОННЫЕ ПИСЬМА.

ТОП-5 ГО ПО КОЛИЧЕСТВУ СОБЫТИЙ, СВЯЗАННЫХ С БОТНЕТАМИ



*** - по части МЦРИАП с учетом подведомственных им организаций**

УЯЗВИМОСТИ ЗОНЫ .KZ

3 220 992
ОБЩЕЕ КОЛИЧЕСТВО ПРОСКАНИРОВАННЫХ IP-АДРЕСОВ В KZ СЕГМЕНТЕ

167 849
КОЛИЧЕСТВО ДОМЕНОВ В ДОМЕННОЙ ЗОНЕ .KZ

Топ-3 по выявленным уязвимым сервисам на интернет-ресурсах:

1. jQuery
2. Nginx
3. PHP

Топ-3 наиболее распространенных сервисов в казахстанском сегменте Интернета:

1. Goahead webserver;
2. jQuery;
3. Nginx.

КОЛИЧЕСТВО ВЫЯВЛЕННЫХ УЯЗВИМЫХ ИНТЕРНЕТ-РЕСУРСОВ
56 013

КОЛИЧЕСТВО ВЫЯВЛЕННЫХ УЯЗВИМЫХ СЕРВИСОВ НА ИНТЕРНЕТ-РЕСУРСАХ
89 377

ВСЕГО ВЫЯВЛЕННЫХ УЯЗВИМОСТЕЙ НА ИНТЕРНЕТ-РЕСУРСАХ
1 033 380

ТОП-5

САМЫХ РАСПРОСТРАНЕННЫХ УЯЗВИМОСТЕЙ НА ИНТЕРНЕТ-РЕСУРСАХ:

1. CVE-2019-11358
2. CVE-2020-11023
3. CVE-2020-11022
4. CVE-2015-9251
5. CVE-2021-3618

КОЛИЧЕСТВО ОТКРЫТЫХ .GIT
134

Наиболее критические уязвимости информационной безопасности, выявленные в ходе мониторинга казахстанского сегмента Интернета:

- Посредством OSINT и специализированной поисковой системы BinaryEdge были обнаружены **230 IP-адресов,** потенциально подверженных **уязвимости с идентификатором CVE-2019-12815**
- Уязвимости CWE-16: Configuration, CWE-521: Weak Password Requirements, CWE-639: Authorization Bypass Through User-Controlled Key *(iDOR)* и CWE-307: Improper Restriction of Excessive Authentication Attempts *(Brute Force)* на ИР ОО «Партия «AMANAT» *(amanatpartiasy.kz)*
- **702 IP-адреса устройств Fortinet,** потенциально подверженных **критической уязвимости CVE-2022-40684.** Выявленные в казахстанском сегменте Интернета IP-адреса являются устройствами Fortinet, эксплуатация уязвимости на выявленных устройствах не проводилась, следовательно, все IP-адреса являются потенциально уязвимыми.
- **98 IP-адресов,** потенциально подверженных **уязвимости идентификатора CVE-2021-44142 удалённому выполнению кода в Samba.**
- **12 серверов Microsoft Exchange,** потенциально подверженных **уязвимости, именуемой ProxyShell с идентификаторами CVE-2021-34473, CVE-2021-34523, CVE-2021-31207.**
- 8 IP-адресов, потенциально подверженных уязвимости идентификатора CVE-2017-12542 - удалённому выполнению кода в HP iLO 4.
- 7 IP-адресов, потенциально подверженных уязвимости идентификатора CVE-2022-22536 - удалённому выполнению кода в продуктах SAP, использующих Internet Communication Manager.
- **75 IP-адресов,** потенциально подверженных **уязвимости идентификатора CVE-2015-1635 - удалённому выполнению кода в продуктах Microsoft.**
- **59 IP-адресов,** потенциально подверженных **уязвимости удалённого выполнения произвольного кода с идентификатором CVE-2022-21971/ Windows Runtime.**
- **7 уязвимых серверов,** использующих **ElasticSearch и находящихся в публичном доступе в Интернете.**
- **16 IP-адресов,** потенциально подверженных уязвимости идентификатора **CVE-2021-43798 *(удаленное выполнение кода в платформе с открытым кодом Grafana).***
- **114 IP-адреса,** потенциально подверженных уязвимости идентификаторами **CVE-2017-7921, CVE-2017-7923, CVE-2021-36260.**
- **25 ИР с внедренными вредоносными ссылками, встроенными в JavaScript.**

В ходе отработки в адрес организаций были направлены уведомления о выявленных уязвимостях и опубликована информация в СМИ с рекомендациями по установке обновления для устранения уязвимостей, а также о проверке наличия индикаторов компрометации (IoC) в сети организации.

APT-ГРУППИРОВКИ

Advanced Persistent Threat

переводится как
развитая устойчивая угроза

APT-группировками принято обозначать злоумышленника, в распоряжении которого имеются специальные знания, соответствующий инструментарий и значительные ресурсы, которые в совокупности позволяют осуществлять целенаправленные кибератаки.
Особенностью целенаправленных атак (APT) является наличие у злоумышленников определенной жертвы, зачастую это крупная компания или государственная организация. Целенаправленные атаки хорошо спланированы и содержат несколько этапов. Результатом атаки может стать закрепление злоумышленников в инфраструктуре жертвы и скрытый сбор данных на протяжении многих месяцев.

Хакерская группировка ToddyCat

ToddyCat - преступную деятельность начали с декабря 2020 года, скомпрометировав сервера Exchange в Тайване и Вьетнаме с помощью неизвестного эксплойта, который привел к созданию веб-оболочки «China Chopper», которая, в свою очередь, использовалась для запуска многоступенчатой цепочки заражения. В этой цепочке выявлен ряд компонентов, в том числе пользовательские загрузчики, используемые для окончательного выполнения пассивного бэкдора Samurai.

- С декабря 2020 г. по февраль 2021 г. группа атаковала ограниченное количество серверов в Тайване и Вьетнаме, принадлежащих трем организациям. Целевые машины, зараженные в период с декабря по февраль, были серверами «Microsoft Windows Exchange»; злоумышленники взламывали серверы с помощью неизвестного эксплойта.
- С 26 февраля до начала марта 2021 г. наблюдалось высокая активность группировки, когда они злоупотребляли уязвимостью «ProxyLogon» для компрометации нескольких организаций в Европе и Азии.

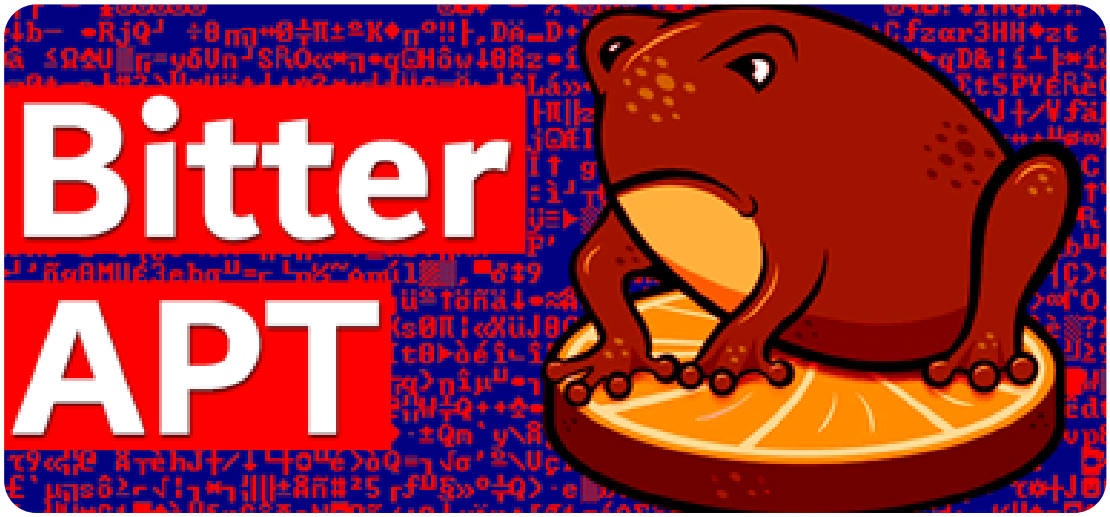
Группировка «ToddyCat» сосредоточила свое внимание на государственные организации и военные структуры, а также военные компании-подрядчики.
ГТС 21 июня 2022 года посредством OSINT *(разведка на основе открытых источников),* аналитической системы «АПК НКЦИБ» и БДУУ были обнаружены 26 IP-адресов в контуре ЕШДИ, которые обращались на зараженные C&C-серверы, которые, согласно отчёту компании «Лаборатории Касперского», используются хакерской группировкой «ToddyCat APT».

Хакерская группировка
ToddyCat

Возможные риски и угрозы:
- RCE-атаки – удаленное выполнение вредоносного кода;
- компрометация системы;
- утечка конфиденциальной информации;
- модификация или удаление важных данных;
- заражение ВПО.

Хакерская группировка Bitter APT *(aka APT-C-08 или T-APT-17)*

Bitter APT - начали свою деятельность с 2013 года, ориентируясь на энергетический, машиностроительный и государственный секторы стран Южной Азии. В своей последней кампании они расширили таргетинг на правительственные учреждения Бангладеша.



Основная деятельность
Bitter APT - шпионаж

Основная деятельность Bitter APT - шпионаж. Злоумышленник обычно загружает вредоносное ПО на скомпрометированные конечные точки со своего хост-сервера через HTTP и использует DNS для установления связи с командованием и управлением. Bitter известен тем, что использует известные уязвимости в средах жертв. Например, в 2021 году исследователи в области безопасности обнаружили, что злоумышленник использовал уязвимость нулевого дня CVE-2021-28310, брешь в системе безопасности Microsoft Desktop Manager. Известно, что Bitter нацелен как на мобильные, так и на настольные платформы. В их арсенале в основном Bitter RAT, загрузчик Artra, SlideRAT и AndroRAT.
Такие кампании наблюдения могут позволить злоумышленникам получить доступ к конфиденциальной информации организации и дать их обработчикам преимущество перед их конкурентами.

Цепочка заражения
ГТС посредством OSINT (разведка на основе открытых источников), аналитической системы «АПК НКЦИБ» и БДУУ были обнаружены 33 IP-адреса, потенциально подверженных угрозе ИБ.

Возможные риски и угрозы:
- RCE-атаки – удаленное выполнение зловредного кода.
- Обход ограничений безопасности.
- Компрометация системы.

Хакерская группировка Cicada APT10

Жертвами Cicada (также известной как APT10) являются правительственные, юридические, религиозные и неправительственные организации во многих странах мира, в том числе в Европе, Азии и Северной Америке. Приписывание этой активности Cicada основано на наличии в сетях жертв пользовательского загрузчика и пользовательского вредоносного ПО, которые, как считается, используются исключительно группой APT.

Для получения доступа к сетям-жертвам группировка использовала известную неисправленную уязвимость

Microsoft Exchange

Для получения доступа к сетям-жертвам группировка использовала известную неисправленную уязвимость Microsoft Exchange. После чего Cicada развертывала различные инструменты, включая специальный загрузчик и бэкдор Sodamaster. Это бесфайловое вредоносное ПО, способное выполнять несколько функций, в том числе уклоняться от обнаружения в песочнице, проверяя ключ реестра или откладывая выполнение; перечисление имени пользователя, имени хоста и операционной системы целевых систем; поиск запущенных процессов, а также загрузка и выполнение дополнительных полезных нагрузок. Он также способен запутывать и шифровать трафик, который отправляет обратно на свой сервер управления и контроля (C&C). Это мощный бэкдор, который Cicada использует с 2020 года.

В этой кампании злоумышленники также сбрасывают учетные данные, в том числе с помощью специального загрузчика Mimikatz. Эта версия Mimikatz удаляет mimilib.dll, чтобы получить учетные данные в виде обычного текста для любого пользователя, который обращается к скомпрометированному узлу и обеспечивает постоянство при перезагрузке.
Посредством OSINT *(разведка на основе открытых источников)* и аппаратно-программного комплекса ГТС были обнаружены **59** IP-адресов, потенциально подверженных угрозе ИБ.

Возможные риски и угрозы:

- RCE-атаки – удаленное выполнение зловредного кода.
- Обход ограничений безопасности.
- Компрометация системы.

Хакерская группировка SideCopy APT

– пакистанская организация, действующая с 2019 года, в основном нацеленная на страны Южной Азии и, в частности, на Индию и Афганистан. Приманки, используемые SideCopy APT, обычно представляют собой архивные файлы, в которые встроен один из следующих файлов: Lnk, Microsoft Publisher или троянские приложения. Эти приманки можно разделить **на две основные группы:**

ПРИМАНКИ, ИСПОЛЬЗУЕМЫЕ SIDECOPY APT, ОБЫЧНО ПРЕДСТАВЛЯЮТ СОБОЙ АРХИВНЫЕ ФАЙЛЫ, В КОТОРЫЕ ВСТРОЕН ОДИН ИЗ СЛЕДУЮЩИХ ФАЙЛОВ: *LNK, MICROSOFT PUBLISHER ИЛИ ТРОЯНСКИЕ ПРИЛОЖЕНИЯ.*

Целевые приманки: приманки специально созданы и предназначены для нацеливания на конкретных жертв. Эта категория очень хорошо подходит для правительственных или военных чиновников:

- Report-to-NSA-Mohib-Meeting-with-FR-GE-UK.zip: этот архивный файл содержит документ Microsoft Publisher, приманка использовалась для нападения на правительственных чиновников Афганистана.

Общие приманки: эти приманки в основном являются общими и использовались в спам-кампаниях для сбора электронных писем и учетных данных, чтобы помочь злоумышленнику выполнять свои целевые атаки. В этой категории наблюдается следующее: (первые три приманки – это те, о которых сообщалось как о «романтических приманках» в отчете Facebook)

- Использование имен девушек в качестве имени архивного файла, такого как «nisha.zip»: Архивные файлы содержат список изображений с расширением «.3d» и приложение с именем «3Dviewer.exe», которое необходимо для выполнения загрузки и просмотра изображений. На самом деле исполняемый файл заражен троянами и будет связываться с серверами-исполнителями для загрузки вредоносных полезных нагрузок.
- «image-random number.zip»: эти zip-файлы содержат вредоносный lnk-файл, который показывает изображение девушки в качестве приманки.
- «Whatsapp-image-random number.zip»: zip-файлы содержат вредоносный lnk-файл, который показывает изображение девушки в качестве приманки.
- «schengen_visa_application_form_english.zip»: архивный файл содержит документ Microsoft Publisher, который загружает форму заявления на получение шенгенской визы на английском языке в качестве приманки. Используется для таргетинга людей, которые хотят поехать в европейские страны.
- «Download-Maria-Gul-CV.zip»: этот архив содержит ссылку, которая загружает резюме в качестве приманки. Имя файла архива обычно имеет вид «Download-Name-FamilyName-CV.zip».

Злоумышленники поддерживают связь с командным сервером через порты, на которые обычно разрешено установление исходящего соединения. Примеры таких портов: TCP:80 (HTTP), TCP:443 (HTTPS), TCP:25 (SMTP), TCP/UDP:53 (DNS). Это помогает обходить обнаружение межсетевыми экранами и выдавать свою деятельность за стандартную сетевую активность. Причем нарушители могут использовать как соответствующий прикладной протокол, закрепленный за конкретным номером порта, так и любой другой протокол прикладного уровня, вплоть до передачи данных по сырым сокетам.

Возможные риски и угрозы.

- RCE-атаки – удаленное выполнение зловредного кода.
- Обход ограничений безопасности.
- Компрометация системы.

DDOS-АТАКИ

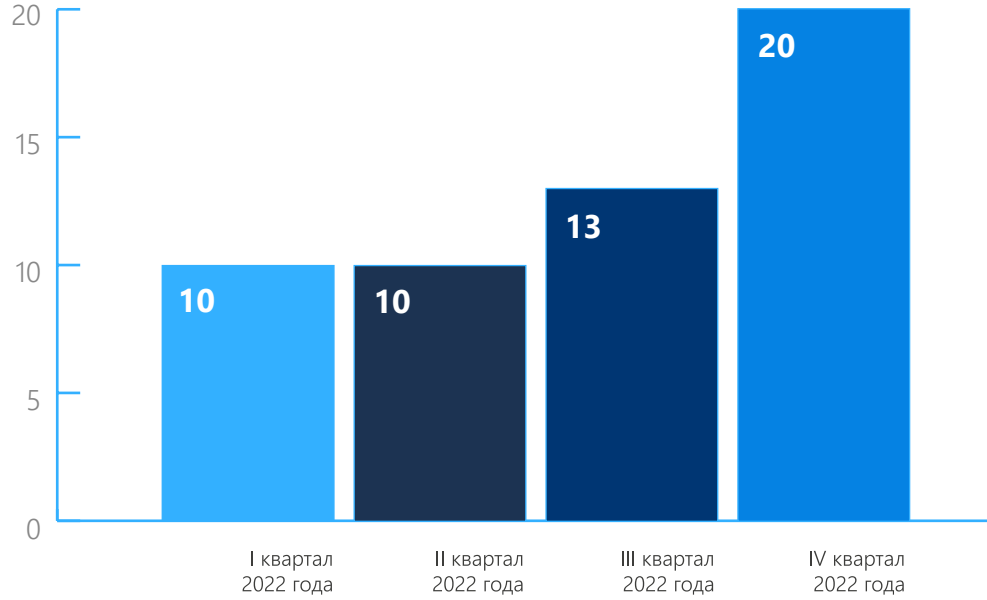
DDOS

Distributed Denial of Service - распределенный отказ в обслуживании

С началом электорального периода АО «ГТС» фиксировало, нарастающие атаки с 28 сентября 2022 года. С целью отражения массовых кибератак средствами защиты «Киберщит» проводились работы по анализу всего сетевого трафика Казахстана.

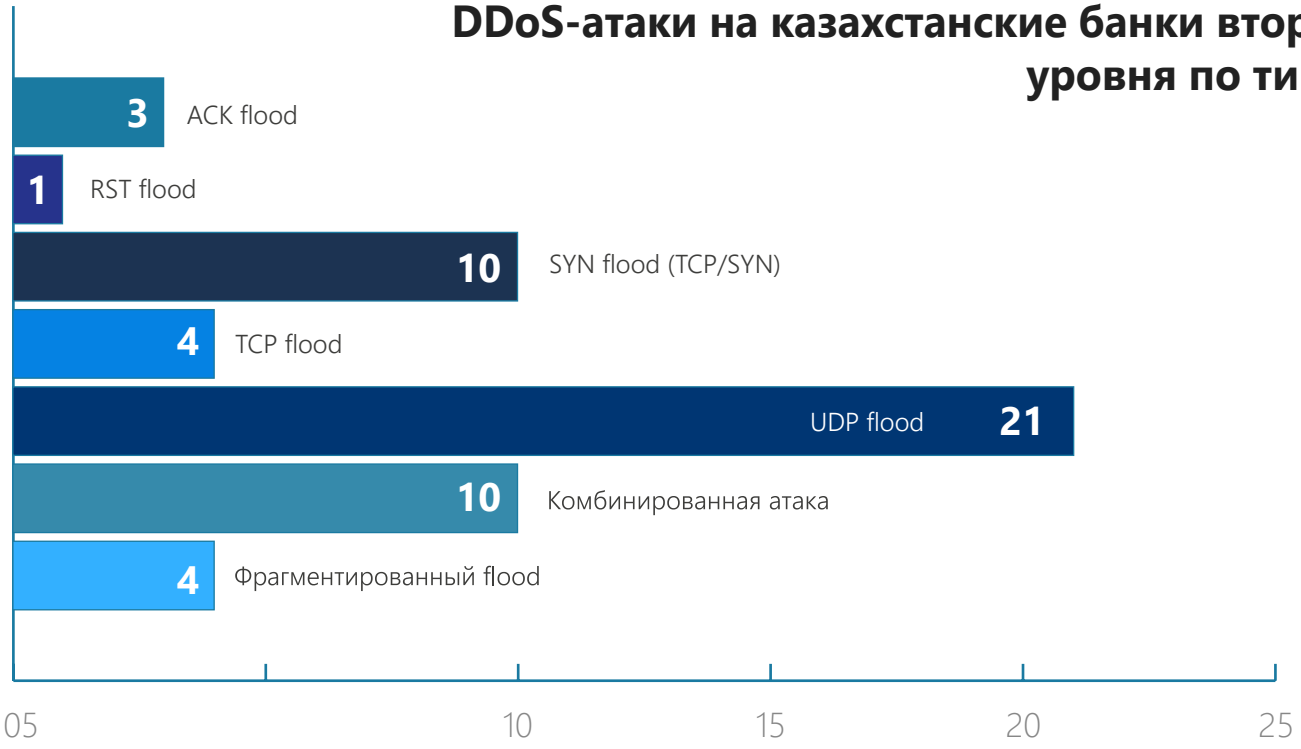
Атаки типа «распределенный отказ в обслуживании» DDoS – это действия, направленные на перегрузку трафиком, когда на атакуемый ресурс отправляется большое количество злонамеренных запросов, из-за чего полностью «забиваются» все каналы сервера или вся полоса пропускания. При этом передача легитимного трафика на сервер затрудняется или становится невозможной.

Количество целенаправленных DDoS-атак на казахстанские банки второго уровня



НАИБОЛЕЕ МОЩНАЯ DDOS-АТАКА ПО ОБЪЕМУ СОСТАВИЛА СВЫШЕ 10 GB/СЕК.

DDoS-атаки на казахстанские банки второго уровня по типам



ТОП-3 ТИПОВ DDOS-АТАК

UDP flood

– сетевая атака, использующая бессеансовый режим протокола UDP. Заключается в отправке множества UDP-пакетов *(как правило, большого объёма)* на определённые или случайные номера портов удалённого хоста, который для каждого полученного пакета должен определить соответствующее приложение, убедиться в отсутствии его активности и отправить ответное ICMP-сообщение «адресат недоступен». В итоге атакуемая система окажется перегруженной: в протоколе UDP механизм предотвращения перегрузок отсутствует, поэтому после начала атаки паразитный трафик быстро захватит всю доступную полосу пропускания и полезному трафику останется лишь малая её часть.
Подменив IP-адреса источников в UDP-пакетах, злоумышленник может перенаправить поток ICMP-ответов и тем самым сохранить работоспособность атакующих хостов, а также обеспечить их анонимность.

SYN flood

– одна из разновидностей сетевых атак, которая заключается в отправке большого количества SYN-запросов *(запросов на подключение по протоколу TCP)* в достаточно короткий срок.
Принцип атаки заключается в том, что злоумышленник, посылая SYN-запросы, переполняет на сервере *(цели атаки)* очередь на подключения. При этом он игнорирует SYN+ACK пакеты цели, не высылая ответные пакеты, либо подделывает заголовок пакета таким образом, что ответный SYN+ACK отправляется на несуществующий адрес. В очереди подключений появляются так называемые полуоткрытые соединения, ожидающие подтверждения от клиента. По истечении определенного тайм-аута эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений. Из-за этого клиенты, не являющиеся злоумышленниками, не могут установить связь, либо устанавливают её с существенными задержками.

Комбинированные атаки

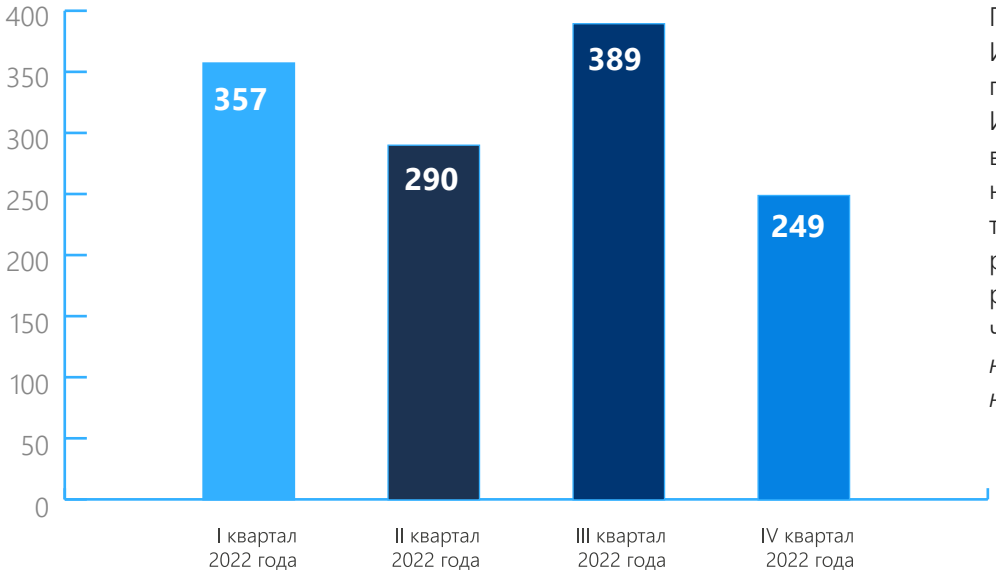
заключаются в применении злоумышленником нескольких взаимосвязанных действий для достижения своей цели.
Большая часть сетей и операционных систем использует IP-адрес компьютера, чтобы определять, тот ли это адресат, который нужен. В некоторых случаях возможно некорректное присвоение IP-адреса *(подмена IP-адреса отправителя другим адресом)*. Такой способ атаки называют фальсификацией адреса или IP-спуфингом.
IP-спуфинг имеет место, когда злоумышленник, находящийся внутри корпорации или вне ее, выдает себя за законного пользователя. Злоумышленник может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам.
Злоумышленник может также использовать специальные программы, формирующие IP-пакеты таким образом, чтобы они выглядели как исходящие с разрешенных внутренних адресов корпоративной сети.
Атаки IP-спуфинга часто являются отправной точкой для других атак. Классическим примером является атака типа «отказ в обслуживании» (DoS), которая начинается с чужого адреса, скрывающего истинную личность хакера. Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложениями или по каналу связи между одноранговыми устройствами.

ТОП-3 ТИПОВ DDOS-АТАК

НЕДОСТУПНОСТЬ ИР

ГТС в круглосуточном режиме проводит мониторинг доступности более 200 ИР. За 2022 год зафиксировано свыше **1 200 событий ИБ, связанных с недоступностью ИР,** находящихся на мониторинге доступности ГТС.

Количество фиксаций событий ИБ типа «Недоступность ИР»



После фиксации недоступности ИР осуществляется выяснение причин, приведших к событию ИБ. В большинстве своем они вызваны разрывами соединений и медленной работой сети, техническими работами на стороне владельца ИР и сбоями в работе программно-аппаратной части *(проблемы работоспособности программного обеспечения и оборудования).*

Топ-5 ИР по общей длительности недоступности

	КОЛИЧЕСТВО ФИКСАЦИЙ НЕДОСТУПНОСТИ	ОБЩЕЕ ВРЕМЯ НЕДОСТУПНОСТИ (ДНЕЙ)	ОБЩЕЕ ВРЕМЯ НЕДОСТУПНОСТИ (МИН)
VCM.UKG.KZ	2	38,7	55736
ZTB.KZ	10	35,1	50613
IGR.KZ	4	27,1	39115
PKREZERV.GOV.KZ	6	26,8	38570
HEARTCENTER.KZ	4	26	37457

ТОП-5 порталов по общей длительности недоступности

	КОЛИЧЕСТВО ФИКСАЦИЙ НЕДОСТУПНОСТИ	ОБЩЕЕ ВРЕМЯ НЕДОСТУПНОСТИ (ДНЕЙ)	ОБЩЕЕ ВРЕМЯ НЕДОСТУПНОСТИ (МИН)
GOSZAKUP.GOV.KZ	10	9,4	13492
PORTAL.KUNDELIK.KZ	28	2,7	3266
QAMQOR.GOV.KZ	7	1,4	1961
EPAY.GOV.KZ	10	1,3	1879
RAILWAYS.KZ	4	1	1347

ФИШИНГОВЫЕ АТАКИ

1 200+ заявок по фишингу зарегистрировано в 2022 году

ФИШИНГ
phishing — от англ. fishing, что значит «рыбалка»

Всего за 2022 год было зафиксировано и отработано более 1 200 заявок, связанных с фишинговыми интернет-ресурсами.
Основными источниками заявок стали Telegram-чат «Информационная безопасность РК» – 83,5% *(1031 заявка)*, веб-платформа НКЦИБ (MISP) – 13,6% *(168 заявок)* и остальные 2,9 % заявок поступили посредством электронной почты и интернет-ресурса cert.gov.kz.

ГТС БЫЛО ЗАРЕГИСТРИРОВАНО СВЫШЕ 1200 ФИШИНГОВЫХ СТРАНИЦ

Большое количество фишинговых атак осуществляется с использованием мошеннических интернет-ресурсов, которые маскируются под легитимные. Подобные атаки представляют собой рассылку ссылок на мошеннические сайты, имитирующие интернет-ресурсы банков второго уровня, популярных компаний, соцсетей, интернет-магазинов и т.д. Злоумышленники рассчитывают на то, что пользователь не заметит подделки и укажет на странице личные данные: реквизиты банковской карты, логин и пароль, номер телефона.
ГТС было зарегистрировано свыше **1 200** фишинговых страниц, доступ к которым был ограничен благодаря взаимодействию с МИОР РК, а также международными командами реагирования на компьютерные инциденты и хостинг-провайдерами. В основном злоумышленниками использовались сайты-опросники для сбора персональных данных потенциальных жертв.

Чаще всего злоумышленники создают фишинговые интернет-ресурсы для проведения мошеннических действий путем сбора персональных данных граждан

МЕЖДУНАРОДНОЕ ВЗАИМОДЕЙСТВИЕ ПО РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Свыше 1000 оповещений направлены в адрес зарубежных организаций 48 государств

ТОП-5 стран с наиболее высоким количеством источников аномальной активности

586 Соединенные Штаты Америки
140 Российская Федерация
71 Китайская Народная Республика
30 Великобритания
22 Вьетнам

ОПОВЕЩЕНИЯ В РАЗРЕЗЕ ТИПОВ ИНЦИДЕНТОВ ИБ

392 Компрометация информации

375 Техническая атака

32 ВПО

Подписано 3 меморандума о взаимопонимании в области кибербезопасности

Национальный CERT Турции

APCERT

Альянс групп реагирования на компьютерные инциденты Азиатско-Тихоокеанского региона

STOP.THINK.CONNECT

STOP | THINK | CONNECT

РЕКОМЕНДАЦИИ

10 простых советов по обеспечению безопасности вашей личной информации. Не забудьте поделиться этими советами со своими коллегами. Таким образом, вы также сможете защитить свою организацию.

1 **Будьте осторожны со ссылками**

Ссылки в электронных письмах – это распространенный инструмент, используемый хакерами, чтобы обманом заставить людей отказаться от своей защищенной информации. Используются в форме банковских выписок, бронирования авиабилетов, электронных писем для восстановления пароля и т. д.

2 **Меняйте пароли.**

Периодически меняйте и используйте уникальные пароли для каждого сайта и учетной записи. Таким образом, если компания, сервисами которой вы пользуетесь, будет взломана, украденные учетные данные не будут работать на других сайтах.

3 **Используйте диспетчер паролей.**

Менеджер паролей — это программа, которая хранит все ваши пароли в одном месте. У пользователя есть один пароль «мастер-ключ» для разблокировки доступа к этим паролям. С менеджером паролей пользователю не придется беспокоиться о запоминании всех своих паролей (LastPass, KeePass, Dashlane, 1Password и Roboform).

4 **Настройте многофакторную аутентификацию**

Без настройки многофакторной аутентификации (MFA) пользователь может получить доступ к своей учетной записи, используя только имя пользователя и пароль. Но MFA добавляет еще один уровень защиты. Для проверки личности пользователя при входе в систему требуется более одного метода аутентификации.

Один из примеров MFA – это когда пользователь входит на веб-сайт и должен ввести дополнительный одноразовый пароль. Этот одноразовый пароль обычно отправляется на адрес электронной почты или на телефон пользователя. Настройка MFA создает многоуровневую защиту, затрудняя несанкционированный доступ к информации пользователя.

5 **Не используйте дебетовые карты в Интернете**

При совершении онлайн-платежей необходимо избегать использования дебетовых карт. Или то, что напрямую связано с пользовательским банковским счетом. Вместо этого предлагается использовать параметры, которые обеспечивают дополнительный уровень защиты между хакерами и пользовательским банковским счетом. Это может быть кредитная карта со страховкой или какой-либо способ оплаты онлайн, например PayPal.

6 **Не сохраняйте информацию о платеже**

Многие веб-сайты позволяют сохранять информацию о кредитной карте, чтобы сделать будущие покупки быстрее и проще. Стоит запомнить, что красть нечего, если кредитная карта пользователя не сохранена на сайте.

7 Держите свои системы в актуальном состоянии

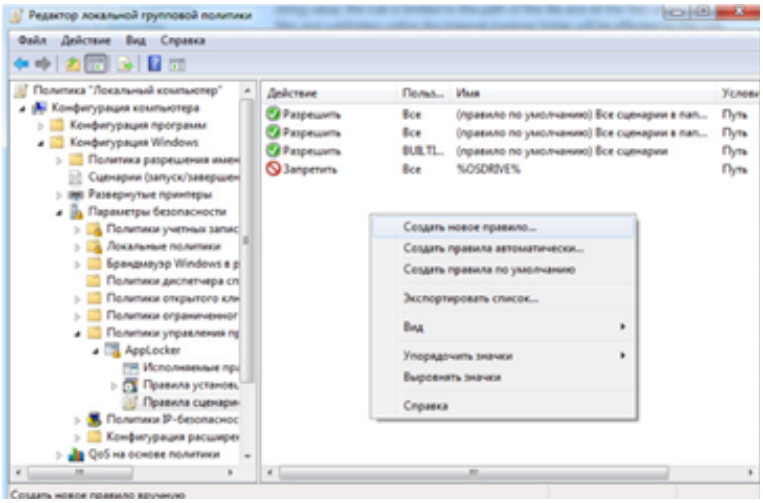
Программное обеспечение пользователя, операционная система и браузер всегда должны быть в актуальном состоянии (обновленные). Обновляя системы пользователя, можно предотвратить использование вредоносных программ.

8 Установите антивирусное программное обеспечение

Вирусы, шпионское ПО, вредоносное ПО, фишинговые атаки и многое другое. Есть так много способов, которыми данные пользователей могут быть скомпрометированы. Установка антивирусного программного обеспечения на пользовательское устройство поможет бороться с большинством этих атак. Необходимо контролировать, чтобы программное обеспечение было активно и в актуальном состоянии.

9 Избегайте ненужных загрузок

Загрузки — это основная тактика, которую используют хакеры для получения доступа к сети пользователя. Чтобы защитить свой компьютер и данные, необходимо ограничить количество скачиваний. Следует избегать любого ненужного программного обеспечения или расширений браузера. А в организации сотрудникам требуется авторизация перед загрузкой из Интернета.



Ограничьте запуск некоторых потенциально опасных типов файлов **(.js, .cmd, .bat, .vba, .ps1)**
Для этого нужно выполнить команду (Win+R) — **gpedit.msc,** далее перейти в раздел К**онфигурация компьютера — Конфигурация Windows — Параметры безопасности — Политики управления приложениями — AppLocker — Правила сценариев** *и с помощью мастера задать новое правило на запрет запуска всех сценариев для всех пользователей, например, на системном диске.*

10 Будьте чрезмерно подозрительны

Хотя многие вещи в Интернете безопасны, лучше перестраховаться. Пользователям необходимо обращать внимание на любые ссылки, которые он нажимает, программные обеспечения, которые он загружает, и посещаемые им сайты.