КОНСПЕКТ
С АКТУАЛЬНЫМИ СПОСОБАМИ СОВЕРШЕНИЯ
КИБЕРВЫМОГАТЕЛЬСТВ

1.ВИДЫ КИБЕРВЫМОГАТЕЛЬСТВ

Все преступления, предусмотренные ст. 208 УК, совершенные с использованием информационно-коммуникационных технологий, можно разделить на три основных вида:

1) связаны с блокированием, модификацией или уничтожением компьютерной информации. При этом в подавляющем большинстве случаев отмечается блокирование мобильных устройств Apple посредством входа на них в предоставленную злоумышленниками под благовидными предлогами учетную запись iCloud, что в последующем позволяет удаленно включить «режим утери» (тем самым заблокировать устройство) либо стереть данные.

Следует отметить, что ранее большая часть предлогов заключалась в онлайн-знакомстве потерпевших с мошенником, представляющимся лицом противоположного пола, у которого сломался телефон и ему необходимо оказать помощь в загрузке каких-либо файлов из облачного хранилища iCloud.

В настоящий момент вектор сместился на рекламу бесплатных игр или приложеиий в социальной сети TikTok, для установки которых необходимо зайти в предоставленный мошенником аккаунт Apple. Потерпевшими в таких случаях выступают подростки, являющиеся активными пользователями указанной социальной сети, - наиболее уязвимая категория граждан.

Также остается актуальным предлог о трудоустройстве, для чего злоумышленники предоставляют соискателю для входа якобы корпоративный аккаунт Apple.

Кроме этого, ряд преступлений данного вида вымогательств связаны с шифрованием файловой системы на серверах предприятий;

2) связаны с угрозой распространения личной информации потерпевших либо иных сведений, которые последние желали сохранить в тайне, преимущественно - фотографий и видеозаписей интимного характера, а также иные личные сведения, которые в большинстве случаев потерпевшие самостоятельно пересылали злоумышленникам, полагая, что общаются с потенциальным партнером для знакомства противоположного пола;

3) связаны с угрозой применения насилия. В данных случаях угроза поступала после того, как потерпевшие пытались дозвониться (либо вели переписку) по абонентским номерам, указанным в анкетах девушек, размещенных на интернет-ресурсах по оказанию сексуальных

услуг.

2.ВЫМОГАТЕЛЬСТВА, СОПРЯЖЕННЫЕ С БЛОКИРОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ APPLE

Прежде всего следует отметить, что механизм блокирования мобильных устройств Apple потерпевших реализуется не путем взлома операционной системы iOS (iPadOS, macOS, watchOS - в зависимости от устройств), а посредством методов социальной инженерии с использованием доверчивости граждан.

Примечание: в дальнейшем для понятности в качестве устройства будем говорить о мобильном телефоне iPhone. Но данная схема актуальна для любого устройства Apple: Mac Book, iPad и др.

Так, злоумышленниками под различными благовидным предлогами вынуждают собеседника выйти из своего аккаунта Apple (iCloud) и войти на iPhone в мошеннический аккаунт, для чего предоставляют логин (адрес электронного почтового ящика) и пароль. С этого момента мобильный телефон жертвы «в руках» вымогателя. Он изменяет пароль от учетной записи, знание которого требуется для выхода из нее, после чего удаленно через облачный сервис iCloud активирует функцию «Найти iPhone», переводя таким образом устройство в режим пропажи, и полностью блокирует его.

Далее потерпевшему приходит сообщение (либо выводится на заблокированном экране), что телефон заблокирован, а для его разблокировки необходимо заплатить деньги. Также зачастую предоставляется контакт в Telegram лица, способного решить этот вопрос (как правило, это и есть злоумышленник, заблокировавший телефон). Характерно, что даже при выполнении требования вымогателя разблокировка устройства в подавляющем большинстве случаев не осуществляется.

Существует несколько основных предлогов, вынуждающих потерпевших войти на своих устройствах в мошеннический аккаунт Apple.

Предлог 1. Реклама бесплатных игр и приложений в социальных сетях и мессенджерах.

Злоумышленники осуществляют размещение рекламы (чаще всего видеоролик в TikTok либо в Telegram), в которой указывается бесплатный способ скачать на iPhone то или иное приложение (AyuGram, Telegram Premium, позволяющие читать удаленные сообщения, забирать «звезды», скрывать статус «онлайн и т.д.), игру («PUBG Mobile», «Standoff 2» и др.) либо мод, получить на свой баланс игровую валюту.

Для установки данных предложений злоумышленники предлагают жертве войти на телефоне в предоставленный ими аккаунт Apple (iCloud). Потерпевшими в таких случаях выступают подростки, являющиеся активными пользователями социальных сетей, - наиболее уязвимая

категория граждан.

Предлог 2. «Сломался телефон». Оказание помощи с файлами из облачного хранилища iCloud.

В данном случае первоначальная коммуникация злоумышленника и жертвы происходит в приложениях либо сайтах для знакомств (Mamba, Masked.love, Twinby, Mail.ru и др.) либо Telegram-чатах («Леонардо Дайвинчик» и др.), где мошенник выступает в качестве лица, противоположного пола, желающего познакомиться. Затем «новый знакомый» переводит общение в мессенджер, где под различными предлогами (например, сломался телефон и необходимо очень срочно скачать какие-либо файлы: курсовую или важные документы) вынуждает потерпевшего зайти в чужую учетную запись Apple на своем iPhone. При этом для большего убедительности присылает заранее заготовленные фотографии разбитого телефона, голосовые сообщения и видеозаписи.

Получив согласие, злоумышленник высылает логин и пароль, а после входа потерпевшим в учетную запись меняет пароль и включает режим пропажи.

Предлог 3. Трудоустройство.

Злоумышленник осуществляет размещение рекламы в сети Интернет о поиск сотрудника на вакансию, как правило связанную с тестированием мобильных приложений для устройств Apple. После удачного «прохождения собеседования» жертве предоставляется логин и пароль для входа в якобы корпоративный аккаунт Apple, который должен использоваться для работы либо загрузки необходимых приложений.

После входа соискателя на своем iPhone в предоставленную учетную запись Apple он оказывается в ловушке. Затем происходят события, аналогичные описанным выше.

Предлог 4. Переход по фишинговой ссылке.

В некоторых случаях «интернет-знакомый» вместо убеждения жертвы войти на своем на телефоне в мошеннический аккаунт Apple, может сбросить ссылку для скачивания приложения, либо входа в облачное хранилище iCloud, где будет предложено ввести логин и пароль от учетной записи Apple уже со стороны потерпевшего. Данная ссылка будет являться фишинговой (поддельной). Введя авторизационные данные своей учетной записи, они сразу же станут известны вымогателю. После смены пароля последний не только заблокирует устройство жертвы, а также получит доступ к его личным данным (фотографии, файлы, заметки, геопозиция, почта и др.), которые синхронизированы в облачном хранилище.

ВАЖНО

Работники сервисных центров не оказывают услуги по восстановлению устройств Apple либо учетных записей iCloud, заблокированных мошенниками. Разблокировать такое устройство

возможно только путем обращения в службу технической поддержки компании Apple, приложив документы, подтверждающие законность его приобретения.

Для этого потерпевший должен обратиться в службу поддержки Apple посредством сервиса Request Activation Lock Support [https://al-support.apple.eom/#/al/agreement] и предоставить: IMEI устройства; доказательства покупки устройства (чек, коробка с IMEI, гарантийный талон); доказательства его «легального» использования потерпевшим (учетная запись Apple потерпевшего, привязанные банковские платежные карточки, телефонные номера и почтовые ящики); обстоятельства противоправного входа (путем введения в заблуждение) в мошеннический Apple ID.

Процесс восстановления через службу поддержки занимает от нескольких дней до недели, при этом устройство может быть сброшено до заводских настроек (все данные удалятся).

Запомните! Настройки iPhone не для игр!

- никогда и не под каким предлогом не входите на своем мобильном устройстве в чужую учетную запись Apple, даже если вас об этом просит друг и тем более - незнакомый человек из интернета;
- никому не сообщайте ваши логин и пароль от аккаунта Apple;
- не переходите по неизвестным ссылкам, пересланным вам незнакомым человеком; не вводите на посторонних сайтах свои логин и пароль от аккаунта Apple iCloud.

Совет родителям, чьи дети используют мобильные устройства Apple.

Для того, чтобы ваш ребенок не смог осуществить ввод логина и пароля предоставленных злоумышленником, достаточно установить родительский контроль. Он никак не ограничивает действия ребенка в функционале мобильного устройства, а только запрещает выйти из учетной записи Apple, а также воспользоваться платежными средствами.

3.ВЫМОГАТЕЛЬСТВА, СВЯЗАНЫЕ С ШИФРОВАНИЕМ ФАЙЛОВОЙ СИСТЕМЫ НА СЕРВЕРАХ ПРЕДПРИЯТИЙ

Мошенническая схема шифрования файлов на серверах предприятий, известная как атака с использованием программ- вымогателей (шифровальщиков), является одной из наиболее опасных киберугроз для бизнеса. Злоумышленники проникают в сеть, чтобы зашифровать критически важные данные и потребовать выкуп за их восстановление.

КАК ПРОИСХОДИТ АТАКА?

Современные атаки шифровальщиков — это не автоматический вирус, а хорошо спланированная операция, управляемая людьми. Ее можно разделить на несколько этапов:

1.Проникновение в сеть. Начальный доступ злоумышленники получают различными способами:

фишинг: массовые или целевые рассылки писем сотрудникам. Например, письмо может маскироваться под накладную от «1С:Предприятие» с вложенным архивом, внутри которого находится вредоносный файл;

атака на удаленный доступ: взлом слабозащищенных точек входа, таких как RDP (протокол удаленного рабочего стола), VPN или серверы с уязвимостями .

использование легитимного ПО: Злоумышленники могут применять легальные программы для мониторинга (например, Mipko Employee Monitor), чтобы оставаться незамеченными и изучать активность сотрудников, перехватывать нажатия клавиш и буфер обмена .

2.Закрепление и разведка. Попав внутрь, злоумышленники не начинают шифрование сразу. Они изучают сеть, ищут ценные данные, повышают свои привилегии, получают доступ к контроллерам домена и, что самое важное, находят и стараются вывести из строя резервные копии. Этот этап может длиться неделями.

3.Подготовка к финальной атаке. Перед запуском шифровальщика преступники часто крадут конфиденциальные данные. Это делается для двойного шантажа: они угрожают не только навсегда заблокировать файлы, но и опубликовать украденную информацию в интернете .

4.Запуск шифрования. В назначенный момент на всех ключевых серверах и рабочих станциях запускается вредоносная программа. Она начинает массово шифровать документы (Office, PDF, базы данных, исходный код и т.д.), часто переименовывая их и оставляя в каждой папке файл с требованием выкупа. Современные шифровальщики также уничтожают теневые копии томов (VSS) и отключают средства восстановления системы, чтобы у жертвы не осталось простых путей отката.

КАК ЗАЩИТИТЬСЯ ОТ ШИФРОВАЛЬЩИКОВ?

Защита должна быть многоуровневой и строиться на принципе «доверяй, но проверяй», а также на готовности к тому, что атака может произойти в любой момент.

Технические меры защиты инфраструктуры.

•Неприкасаемые резервные копии (правило 3-2-1). Это самый главный пункт. У вас должно быть как минимум три копии данных, на двух разных носителях, и одна копия обязательно должна храниться вне основной инфраструктуры (офлайн), чтобы злоумышленники не могли до нее добраться. В облачных средах стоит использовать неизменяемые (immutable) резервные копии, которые нельзя изменить или удалить даже при компрометации учетной записи администратора.

•Принцип минимальных привилегий. У сотрудников должен быть доступ ровно к тем данным, которые необходимы для работы, и не больше. Административные учетные записи должны использоваться

только для выполнения конкретных задач.

•Многофакторная аутентификация (MFA). Обязательно включите MFA везде, где это возможно: для доступа к почте, VPN, облачным сервисам и, конечно, к консолям администрирования серверов.

•Сегментация сети. Критически важные серверы (файловые, резервного копирования, базы данных) должны находиться в отдельных виртуальных сетях (VLAN) с жесткими правилами доступа. Это не даст атаке с зараженного компьютера бухгалтера быстро перекинуться на все хранилища.

•Обновление ПО и политики запуска. Своевременно устанавливайте обновления безопасности. Используйте белые списки приложений (AppLocker, WDAC), чтобы запретить запуск неподписанных или неразрешенных программ, включая неизвестные шифровальщики .

ЧТО НЕ НАДО ДЕЛАТЬ РАБОТНИКАМ ПРЕДПРИЯТИЙ? ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ.

Самая совершенная защита может рухнуть из-за одной ошибки сотрудника. Поэтому персоналу категорически нельзя:

1.переходить по подозрительным ссылкам и открывать вложения в письмах от незнакомцев, даже если они выглядят как документы от контрагентов или госорганов;

2.использовать слабые пароли (типа "password 123", "Qwerty" или "1С") и записывать их на стикерах, приклеенных к монитору;

3.подключать к рабочим компьютерам личные или найденные USB-накопители, которые могут быть заражены;

4.игнорировать необычное поведение компьютера (резкое замедление, невозможность открыть файлы, появление странных файлов с требованием выкупа). В такой ситуации нужно немедленно отключить компьютер от сети и сообщить в 1Т-отдел;

5.передавать логины и пароли коллегам по телефону или в мессенджерах.

ЧТО ДЕЛАТЬ, ЕСЛИ ФАЙЛЫ УЖЕ ЗАШИФРОВАНЫ?

Если беда все-таки случилась, главное правило — не паниковать и не платить выкуп. Платеж не гарантирует возврат данных и лишь финансирует дальнейшие атаки преступников.

План действий должен выглядеть следующим образом.

1.Изолировать зараженные системы. Немедленно отключите зараженные компьютеры и серверы от сети (физически выдерните сетевой кабель). Это может остановить распространение шифрования на другие устройства.

2.Сообщить о проблеме. Немедленно уведомите руководство и отдел информационной безопасности. Если в компании есть регламент по реагированию на инциденты, следуйте ему.

3.Оценить ущерб и начать восстановление. Вместе со специалистами определите, какие системы затронуты. Если у вас есть чистые, не затронутые атакой резервные копии, можно начинать процесс восстановления. Для этого потребуется полностью переустановить ОС на зараженных машинах и только после этого восстанавливать данные.

4.Обратиться в милицию. Это не просто рекомендация, а важный шаг для официальной фиксации преступления. Представитель компании (руководитель или ответственный за информационную безопасность) должен написать заявление. Необходимо предоставить любые материалы, которые могут помочь расследованию: переписку с вымогателями (если она была), IP-адреса, образцы зашифрованных файлов (для последующей передаче экспертам) и файлов с требованиями.

СЛЕДУЕТ ПОМНИТЬ: атаки шифровальщиков - это вопрос не «если», а «когда». Поэтому ключ к информационной безопасности предприятия - надежные изолированные бэкапы, обученные сотрудники и отработанный план действий на случай инцидента.

4.ВЫМОГАТЕЛЬСТВА, РАСПРОСТРАНЕНИЯ ПОТЕРПЕВШИХ ЛИБО СВЯЗАННЫЕ С УГРОЗОЙ ЛИЧНОЙИНФОРМАЦИИ ИНЫХ СВЕДЕНИЙ, КОТОРЫЕ ПОСЛЕДНИЕ ЖЕЛАЛИ СОХРАНИТЬ В ТАЙНЕ

При данном виде вымогательств в подавляющем большинстве случаев объектом преступления являются фотографии и видеозаписи интимного характера потерпевшего, переписка на сексуальную тему либо иная компрометирующая информация.

Первоначальная коммуникация злоумышленника и жертвы происходит в приложениях либо сайтах для знакомств (МашЬа, Masked.love, Twinby, Mail.ru и др.) либо Telegram-чатах («Леонардо Дайвинчик» и др.), где мошенник выступает в качестве лица, противоположного пола, желающего познакомиться. Затем общение довольно быстро приобретает сексуальный подтекст. «Новый знакомый» предлагает обменяться интимными фотографиями. При этом для большего убедительности присылает заранее заготовленные якобы свои фотографии либо видео в обнаженном виде.

В случае, если жертва «повелась» на данное предложение и сбросила свои интимные фотографии или видео, злоумышленник их сохраняет. При этом отправление самоуничтожающихся сообщений не поможет, так как экран всегда можно сфотографировать другим устройством. Одновременно с этим вымогатель собирает информацию о жертве в сети Интернет: находит страницы в социальных сетях, анализирует данные из открытых источников, узнает круг друзей и родственников, место работы. Затем злоумышленник сообщает, что распространит имеющиеся у него интимные фотографии потерпевшего среди его друзей и знакомых либо выложит в открытый доступ, если ему

не заплатать за их нераспространение.

Если же в ходе интернет-переписки вымогателю не удалось получить интимные изображения жертвы, он может изготовить их с помощью различных фоторедакторов, используя фотографии собеседника из его социальных сетей. Также злоумышленник может угрожать оглаской состоявшейся переписки на сексуальные темы, дополнительно сообщив, что является несовершеннолетним, таким образом намекая о возможности привлечения жертвы за «совращение малолетнего».

В некоторых случаях «интернет-знакомый» может сбросить фишинговую ссылку, например, для просмотра фото в облачном хранилище либо его видео на различных стриминговых сервисах. Перейдя по ссылке и введя свои данные (как правило, абонентский номер и полученный код-подтверждение) злоумышленник получает доступ к мессенджеру жертвы и его социальным сетям. В таком случае вымогатель получает доступ ко всем контактам и перепискам потерпевшего, а при наличии в них интимных фото или видео (например, при общении с другими девушками) либо иной компрометирующей информации, использует ее по вышеописанному принципу. В данном случае ситуация усугубляется тем, что злоумышленник видит все реальные контакты жертвы, а также может использовать ее личные учетные записи для совершения иных мошеннических действий (просить одолжить деньги, перевести средства на благотворительный сбор и т.д.).

Запомните! Настройки iPhone не для игр!

•никогда не отправляйте свои интимные фотографии и видео незнакомцам из интернета;

•не оставляйте в сети Интернет о себе личную информацию и не делитесь с ней с незнакомцами;

•скройте данные о себе в настройках конфиденциальности в социальных сетях и мессенджерах;

•не переходите по неизвестным ссылкам, пересланным вам незнакомым человеком; не вводите на посторонних сайтах свои личные данные и коды из сообщений.

ТАКЖЕ СЛЕДУЕТ ПОМНИТЬ, что изготовление и распространение порнографических материалов или предметов порнографического характера влечет за собой привлечение к уголовной ответственности по ст. 343 Уголовного кодекса Республики Беларусь с применением наказания вплоть до двух лет лишения свободы.

5.ВЫМОГАТЕЛЬСТВА, СВЯЗАННЫЕ С УГРОЗОЙ ПРИМЕНЕНИЯ НАСИЛИЯ, ПОСЛЕ ПОСЕЩЕНИЯ САЙТОВ ПО ОКАЗАНИЮ СЕКСУАЛЬНЫХ УСЛУГ

Злоумышленники на различных сайтах по оказанию сексуальных услуг размещают анкеты девушек, в которых зачастую в качестве

контактного указывают абонентский номер белорусского оператора мобильной связи.

Потерпевшие, находясь в поисках подобных услуг, безрезультатно пытаются дозвониться по указанному в анкете абонентскому номеру (трубку никто не снимает).

В последующем, как правило на следующий день, потерпевшим поступает телефонный звонок, в ходе которого лицо с выраженным кавказским акцентом в голосе сообщает, что по причине звонка произошло «блокирование кассы» (либо иные причины), ввиду чего «девушки не могут работать». В ходе звонка злоумышленник предлагает решить вопрос «тихо-мирно», пополнив баланс «кассы», тем самым ее разблокировать. В дальнейшем происходит давление в сторону жертвы и склонение к переводу все больших сумм денежных средств под различными предлогами, в том числе высказываются угрозы жизни и здоровью потерпевшего либо его близких родственников.

В последующем общение переводится в мессенджер, куда сбрасываются реквизиты, на которые необходимо перечислить денежные средств (как правило, p2p переводы). Туда же потерпевшие сбрасывают электронные чеки как подтверждение о переводе денежных средств.

В некоторых случаях на звонки или сообщения потерпевших при посещении интернет-сайтов отвечает якобы девушка и договаривается о встрече, для чего требуются предоплаты в качестве гарантии. В действительности никакой девушки' не существует, а злоумышленники просто имитируют женский голос. После совершения данной мошеннической схемы также следуют звонки по вышеописанному принципу.

СЛЕДУЕТ ПОМНИТЬ! Реклама услуг сексуального характера в Республике Беларусь запрещена. Отказ от подобного досуга не только убережет ваше здоровье, но и деньги.