Zoombombing: работа над ошибками и урок для конкурентов

Новое время неожиданно жёстко и уверенно начало диктовать нам свои правила игры и ведения бизнеса. И если совсем недавно видеоконференции и видеосовещания были скорее исключением, чем правилом, то сегодня приложения для удалённого общения бьют все рекорды скачивания. В интернет перемещаются не минуты, а часы, десятки и сотни часов конфиденциальных переговоров. Таких, за содержание которых которые асы промышленного шпионажа готовы платить любые деньги. А потому интерес злоумышленников всех мастей к системам видеоконференцсвязи растёт прямо пропорционально количеству скачиваний.

Да и досужим хакерам есть где разгуляться. Ещё бы. Представьте себе, сидят за круглым столом (у мониторов, то есть) строгие дяди-тёти, обсуждают что-то. И вдруг:

> "Здрасьте! Я тут гулял, гляжу, дверь открыта, ну и зашёл на огонёк. Как поживаете?".

Впрочем, это забава для школьников, которые всегда любили сорвать урок. А уж урок в онлайне… О, мечта юного хулигана-хакера. Именно такие эффектные визиты на чужие конференции и получили название Zoombombing, или зумбомбёжка.

Рекордный спрос на фоне пандемии

О такой популярности приложений для видеоконференций разработчики ещё в конце прошлого декабря даже мечтать не могли. Но уже в январе, когда на карантин ушёл Китай, количество скачиваний начало резко увеличиваться. Февраль, март и апрель, когда следом за Китаем на "удалёнку" начал переходить весь мир, сделали этот рост лавинообразным. К примеру, по данным Рейтер, приложение для видеоконференций Webex от Cisco зарегистрировало в марте рекорд – 324 миллиона пользователей. В 2,5 раза выросло количество пользователей в Южной Америке, в 3,5 раза – в Азиатско-Тихоокеанском регионе, в четыре раза – в Европе.

Webex и конкуренты, платформы для видеоконференций – Zoom, Microsoft Corp и другие используются во всем мире для любого группового общения от виртуальных классов и деловых встреч до церковных служб. Людям необходимо общаться и во время пандемии, и виртуальные встречи – единственный способ встретиться во время карантина.

Главные направления роста, по данным экспертов Cisco, – образование и телемедицина. В марте в Webex было проведено около 73 миллионов видеоконференций. Итоги апреля пока не подведены, но вероятнее всего, на фоне всеобщего карантина количество скачиваний будет увеличиваться..

Рекордный рост показал Zoom, ежедневная аудитория которого в марте взлетела с 10 до 200 миллионов.

Скандал с ZOOM, как предвестник грозы

Невиданный и нежданный "коронавирусный" взлёт популярности Zoom очень быстро вылился в грандиозный скандал.

Вынужденные работать из офисов, люди оценили возможности, предоставленные Zoom, но, судя по всему, недооценили его безопасность, и уже в начале апреля в сеть были выложены тысячи видеозвонков, сделанных с помощью Zoom. В открытом доступе оказались как деловые конференции и переговоры, так и личные, глубоко интимные диалоги.

Все желающие могли посмотреть сеансы психотерапии, телемедицинские встречи, с указанием телефонных номеров были выложены совещания в различных компаниях, причём, на этих совещаниях обсуждаются финансовые и технологические отчёты, явно не предназначенные для публикации. Все эти видео были записаны с помощью ПО Zoom и сохранены в отдельном онлайн-хранилище со свободным доступом.

Одновременно у взломщиков появилась мода непрошенными являться на закрытые встречи, школьные уроки, конфиденциальные переговоры – Zoombombing.

Руководство Zoom честно признало существование проблем, и активно взялось за усиление защиты своих абонентов, но заверения и обещания мало кого убедили, и руководство Google, МИД Германии, Тайваня, Индии и других стран предупредили граждан о том, что с Zoom лучше пока не связываться.

За что поплатился Zoom ?

Спрос на все виды приложений для видеообщения растёт во всём мире по мере распространения коронавируса. Сегодня покупают и скачивают всё, от разработок с простым доступом,

предназначенных для школьников и обычных пользователей – это, к примеру, House Party, Google Hangouts или Zoom, до бизнес-ориентированных Cisco, Webex, Microsoft Teams, – пишет Рейтер. Но при всём богатстве выбора никто не может быть застрахован от утечек или "зумбомбёжки".

В конце марта разгорелся скандал вокруг Houseparty. Пользователи начали массово удалять приложения, когда в соцсетях и и на форумах появились массовые жалобы на то, что после загрузки Houseparty на смартфонах были взломаны другие приложения.

Разработчик приложения отклонил все обвинения и предложил вознаграждение в миллион долларов тому, кто найдёт инициаторов клеветнической кампании и докажет их вину.

Если же говорить о Zoom, то эксперты считают, что главная причина проблем приложения – взрывной рост популярности, к которому не были готовы и сами владельцы и разработчики. В один момент Zoom превратился из бизнес-инструмента телеконференций в глобальную видеовстречу.

> "Если раньше Zoom применяли только закрытые группы, то теперь в видеочат приходится приглашать и незнакомых людей, с которыми по каким-то причинам нужно переговорить. Это очень серьёзные изменения", – считает бывший директор по безопасности Facebook Inc, Алекс Стамос, который теперь сотрудничает с Zoom в качестве внешнего консультанта.

С тех пор, как приложением начали пользоваться не десятки, а сотни миллионов человек, исследователи безопасности обнаружили ошибки в коде, обмен пользовательскими данными с Facebook, отсутствие сквозного шифрования и маршрутизацию части трафика через Китай.

Конфиденциальность и безопасность. Как исправился Zoom

Эксперты считают, что инцидентов с "зумбомбёжкой" можно было избежать, подумай организаторы встреч о конфиденциальности заранее. Достаточно было ввести пароли для входа в чат или сохранение практики рассылки приглашений в узких группах, и "зумбобардировщики" не смогли бы заявиться на собрании с торжествующим: "а вот и я, не ждали?".

После скандала Zoom обновил программное обеспечение и предоставил организаторам возможность проводить закрытые встречи, ограничивать возможности, приглашать и удалять участников. Кроме того, у Facebook отозвали доступ к данным приложения.

Разработчики советуют организатору конференции давать персональное разрешение каждому, кто хочет присоединиться к чату и не предоставлять доступ незнакомым и сомнительным гражданам, приславшим запросы на участие.

Эксперт в вопросах кибербезопасности Даниэль Катберт считает, что Zoom допустил серьезные, но не уникальные ошибки, которые, к счастью, можно достаточно быстро исправить. И главное, что Zoom быстро отреагировал на ситуацию и исправил ошибки.

К чему приводит обман потребителей

Конфиденциальность и безопасность. Казалось бы, разницы между этими понятиями и нет, особенно если речь идёт о защите приложений для ВКС. Между тем, если речь идёт о личных разговорах, то абонентов волнует конфиденциальность. Им очень важно, чтобы содержание личных разговоров не стало достоянием злоумышленников. Обеспечить конфиденциальность, по мнению экспертов, можно с помощью паролей и ограничений на доступ. Другое дело – корпоративные клиенты, которых волнует проблема шифрования и защиты бизнес-информации.

Если первая категория абонентов не понесла от утечки репутационных и финансовых потерь, то вторая могла пострадать очень серьёзно. Иногда одно слово, сказанное на закрытом совещании в банке, может стоить миллионы.

Zoom привлек лучших специалистов отрасли в области безопасности, устранил практически все погрешности, избавился от маршрутизации через Китай, но руководству компании пришлось признать, что клиентов намеренно ввели в заблуждение, обещая сквозное шифрование. Именно этот обман и стал причиной того, что многие корпорации отказались после скандала от услуг Zoom.

"Мы – хорошие, мы утечек не допустим"

...в один голос закричали, после скандала с Zoom, представители всех крупных платформ для видеоконференцсвязи.

Каким бы высоким ни был спрос на приложения для ВКС, конкуренция на рынке не ослабевает. Отхватить кусок пожирнее стараются все, а потому все как один уверяют, что тайны пользователей будут защищены сквозным шифрованием, что никто и никогда не сможет взломать, что уж у них-то

"зумбомбёжки" не будет точно.

Но эксперты предупреждают: даже если в опции в системе ВКС предусмотрено сквозное шифрование, не всё так просто. При сохранении данных сеанса, стенограммы вызовов, записи вызовов и звонках со стационарных телефонов, сквозное шифрование не поддерживается, так что утечек избежать не получится.

Cisco, ВКС которой в марте пользовались 324 миллиона человек, уверяет, что WebEx надёжно защищена шифрованием.

> "Мы не используем ваши данные, не храним ваши переговоры, не продаём ваши данные рекламным агентствам. WebEx – надёжный инструмент для безопасного общения", – уверяет пользователей вице-президент Cisco Джонатан Дэвидсон.

Microsoft Team, с 44 миллионами пользователей тоже предлагает продукты, защищённые сквозным шифрованием. В полной надёжности уверяют и другие разработчики приложений для бизнес-конференций.

Но насколько в самом деле надёжна защита? Смогут ли конкуренты обойти маститых лидеров рынка, предлагая интересные цены и уникальный пакет опций? Удастся ли им обеспечить конфиденциальность и безопасность при том, что квалификация и аппетиты хакеров растут пропорционально количеству видеоконференций в прямом эфире? Покажет время. Но почему-то мне кажется, что история Zoom – это первый громкий скандал, который дал имя новому явлению, и "зумбомбёжки" могут продолжиться.