ОСОБЕННОСТИ ЗЛОСТНОГО ZOOM-ТРОЛЛИНГА И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ЕМУ

FEATURES OF THE EVIL ZOOM-TROLLING AND METHODS TO COUNTER WITH IT

Козлов Михаил
Ph.D. Директор Института интеграции и профессиональной адаптации, вице-президент по интеллектуальным информационным технологиям Израильской независимой академии развития науки, Нетания, Израиль.
Email: 19mike19k@gmail.com, тел: +(972)527 052 460,

Kozlov Michail
Ph.D. Director of Institute Integration and Professional Adaptation, Vice President, Intelligent Information Technology, Israel Independent Academy of Development of Science. Netanya, Israel.
Email: 19mike19k@gmail.com, tel: +(972)527 052 460,

Аннотация. Представлен анализ ситуации, связанной со злостными атаками на средние по численности мероприятия, проводимые через ZOOM, особенности такого троллинга и некоторые рекомендации по противодействию этому.

Ключевые слова: ЗУМ-мероприятия, ЗУМ-атаки, интернет, тролль, психопатические наклонности, информационные троллинг-потоки.

Abstract. An analysis of the situation associated with malicious attacks on medium-sized events carried out through ZOOM, the features of such trolling and some recommendations for countering this is presented.

Key words: ZOOM events, Zoombombing, Internet, troll, psychopathic inclinations, informational trolling streams.

На фоне пандемии коронавируса резко выросла потребность в использовании приложения Zoom, как для возможности удалённой работы и дистанционного обучения, так и для восстановления и поддержания общения между собой большого количества людей и Zoom де-факто стал социальной платформой для эпохи коронавируса [1]. Как было отмечено в [2] “Человек как существо социальное, не может без психологических и, следовательно, физических нарушений переносить изоляцию. Особенно остро негативные последствия изоляции отражаются на людях пожилого возраста, которые к тому же часто больны и одиноки”. И налаживание комфортного интернет-общения с помощью ZOOM для такой категории населения является актуально значимой социальной задачей.

В такой ситуации всякое нарушение общения с помощью ZOOM воспринимается негативно и особенно это касается злостных проявлений троллинга в ZOOM, связанных с хакерскими атаками, несущими оскорбительные сообщения и ролики. В связи с этим возникла потребность разобраться в особенностях ZOOM-троллинга и в методах противодействия таким атакам. И, возможно, есть смысл рассмотреть отдельно противодействию злостному ZOOM-троллингу при проведении средних по численности мероприятий до 100 человек.

ZOOM-троллинг новое явление в интернете и имеет как свои традиционные основы [3], так и свои отличительные черты [1]. В зависимости от направлений видеоконференций

ZOOM-атаки (Zoombombing) могут иметь свои особенности, при этом, как отмечено в [1], для того чтобы помешать или даже сорвать видеоконференции ZOOM-тролли часто используют шокирующие образы и ненормативную лексику.

Из анализа наблюдавшихся событий ZOOM-троллинга при средних по численности ZOOM-мероприятий, проводимых для общения пожилых людей, складывается мнение, что проводимые ZOOM-атаки не связаны с детскими шалостями и их производит один или в крайнем случае два-три организованных в группу человека.

На основании проведенного анализа и материалов, изложенных в [4] можно предположить, что организатором ZOOM-троллинга является технически грамотная личность с психопатическими наклонностями. Для реализации ZOOM-атаки этот человек может использовать несколько компьютеров или других гаджетов с доступом к интернету и таким образом может осуществлять по типу стаи боевых дронов ZOOM-атаки разными источниками одновременно или последовательно. При этом может использоваться два канала воздействия на участников ZOOM-встречи – звукового и визуального.

Информационные троллинг-потоки для более эффективного их воздействия могут быть заранее записаны и запускаться одним человеком по разным каналам. При этом ZOOM-тролль может маскировать свои действия, например, под детские гнусные шалости, как это было в анализируемых событиях. То, что это не действия дети, а целенаправленные действия взрослого человека уже не вызывает сомнений при анализе подобных ситуаций. При этом, не надо исключать того, что за человеком с психопатическими наклонностями или организованной группой лиц может стоять заинтересованные в ZOOM-атаках интересанты.

Последовательность ZOOM-атак показала, что методы ZOOM-троллинга совершенствуются и в начале атаки уже начали использовать мощный звуковой сигнал в виде белого шума, который лишает возможности организаторам встречи вести переговоры по координации противодействия. Очевидно, к такому началу ЗУМ-атак надо быть готовым и быстро находить, и удалять такой источник, а далее методично, последовательно выявлять инициатора ZOOM-атак по звуковым и видео каналам.

По-видимому, нецелесообразным является массовое отключение и удаление тех, кто может вызывать малейшее подозрение у ведущего техническое сопровождение ZOOM-мероприятия. Это может дать сиюминутный эффект, но не позволит выявить источник атак. Кроме того, вызовет обиду у незаслуженно удаленных и, зачастую, еще неопытных в работе с ZOOM и слабо владеющих им. Более того, организатор атак, скорее всего, останется на ZOOM-мероприятии и затаится. И будет накапливать опыт для следующих ZOOM-атак.

Весьма полезным может оказаться предварительный фейсконтроль всех входящих на ЗУМ-мероприятия и повторный фейсконтроль во время атаки. После входного фейсконтроля участники мероприятий могут отключать свои видеокамеры.

Для малых и хорошо владеющих работой через ZOOM людей можно использовать систему паролей при вхождении на ZOOM-мероприятие. Но этот весьма эффективный метод сложно будет применять для случайно организованных групп людей.

В качестве превентивных мер по предупреждению атак ZOOM-троллей могут быть полезными пять, приведенных в [5] советов:

1. не использовать свой личный идентификатор встречи;
2. использовать пароль встречи;
3. использовать функцию зала ожидания Zoom. Когда включена комната ожидания для собрания Zoom, то каждый подключающийся пользователь помещается в очередь, из которой организатор может не впустить на конференцию нежелательных лиц;
4. отключить звук и отключить видео для участников встречи. Отключение видео для всех, кроме организатора, не позволит участникам встречи выводить на экран непристойной контент. Отключение звука для всех участников должно быть выполнено организатором после начала собрания;

5. отключить общий доступ к экрану для всех, кроме организатора встречи.

Заключение

Представленный анализ рассматривается как предварительный, который может быть полезным при выработке практических решений по борьбе с злостными ZOOM-троллями. Для повышения эффективности противодействия ZOOM-атакам и выявлению ZOOM-троллей, по-видимому, необходимо объединять усилия как специалистов в области информационных технологий, системных аналитиков, организаторов массовых мероприятий, психологов и психиатров, так и госструктур.

БИБЛИОГРАФИЯ

1. Taylor Lorenz; Davey Alba. Zoombombing Becomes a Dangerous Organized Effort. The New York Times. April 7, 2020
2. Лернер Л. Возможности ZOOM в преодолении негативных последствий самоизоляции у пожилых ученых-репатриантов. 7.09.2020. Сайт Института интеграции и профессиональной адаптации http://netanyascientific.com
3. Козлов М. Интернет-троллинг и как с ним бороться, родимым. NIZI.co.il / Наука и жизнь Израиля. 21.11.2015
4. Sorokowski P., Kowal M., Zdybek P., Oleszkiewicz A. Are Online Haters Psychopaths? Psychological Predictors of Online Hating Behavior. Front. Psychol., 27 March 2020. https://doi.org/10.3389/fpsyg.2020.00553
5. Brandon Vigliarolo. How to prevent Zoom bombing: 5 simple tips – TechRepublic. April 3, 2020. https://www.techrepublic.com ›