Почему жертва взлома пытается спрятаться от поисковиков?

26 июня компания TeamViewer – это программное обеспечение для удалённого доступа и управления через интернет. С его помощью можно подключаться к удалённым компьютерам, чтобы оказать техническую поддержку, провести презентацию или выполнить другие задачи. TeamViewer позволяет передавать файлы, чатиться и даже проводить видеозвонки. Это удобное средство для работы с удалёнными устройствами, которое широко используется как в бизнесе, так и среди обычных пользователей." data-html="true" data-original-title="TeamViewer" >TeamViewer сообщила об обнаружении аномалии в своей внутренней корпоративной IT-среде. Была активирована группа реагирования и начато расследование совместно с ведущими мировыми экспертами по кибербезопасности. Были также предприняты необходимые меры по устранению последствий инцидента.

TeamViewer уверяет, что корпоративная IT-среда полностью изолирована от среды продуктов компании, и на данный момент нет свидетельств того, что данные клиентов пострадали в результате инцидента. Подробности о том, кто мог стоять за взломом и каким образом он был осуществлен, не разглашаются, но TeamViewer обещает предоставлять обновления по мере поступления новой информации.

Однако, несмотря на заверения в прозрачности, страница с заявлением о взломе содержит метатег <meta name= "robots" content="noindex">, который препятствует индексации документа поисковыми системами, что делает его труднодоступным для пользователей.

Первое сообщение о взломе появилось на Mastodon – это децентрализованная социальная сеть, основанная на открытом исходном коде. Она была создана в 2016 году разработчиком Эжени Рохком де Беллабром в ответ на проблемы приватности и контроля контента в главных социальных медиа платформах, таких как Twitter и Facebook.<br /> <br /> В Mastodon нет одного центрального сервера. Вместо этого он состоит из множества независимых серверов, называемых «инстанциями». Это означает, что каждый сервер управляется его администраторами, которые могут устанавливать свои собственные правила и политики модерации.<br /> <br /> Пользователи Mastodon могут создавать учетные записи на любой инстанции и взаимодействовать с другими людьми на любой другой инстанции. Это делает платформу более открытой и гибкой, чем традиционные социальные сети." data-html="true" data-original-title="Mastodon" >Mastodon от ИБ-специалиста Jeffrey, который поделился частью оповещения от команды NCC Group – компания, занимающаяся обеспечением информационной безопасности, штаб-квартира которой

находится в Манчестере, Великобритания. В сферу услуг NCC входит депонирование и проверка программного обеспечения, консалтинг в области кибербезопасности и управляемые услуги. NCC Group обслуживает более 15 000 клиентов по всему миру." data-html="true" data-original-title="NCC Group" >NCC Group, размещённого на Dutch Digital Trust Center — веб-портале, который используется правительством, экспертами по безопасности и голландскими корпорациями для обмена информацией об угрозах кибербезопасности. В оповещении говорится, что платформа TeamViewer подверглась взлому со стороны Усовершенствованная постоянная угроза (Advanced Persistent Threat, APT) — это скрытая угроза, за которой обычно стоит национальное государство или спонсируемая государством группировка, которая получает несанкционированный доступ к компьютерной сети и остается незамеченной в течение длительного периода времени. <br> <br> В последнее время этот термин может также относиться и к нефинансируемым государством группам, осуществляющим, тем не менее, крупномасштабные целевые вторжения для достижения определённых целей. <br> <br> Мотивы таких субъектов угрозы обычно носят политический или экономический характер." data-html="true" data-original-title="APT" >APT-группы.

Оповещение Dutch Digital Trust Center

NCC Group предупредила, что из-за широкого использования программы это оповещение было распространено среди клиентов TeamViewer. Кроме того, сообщество Health-ISAC также сообщило, что услуги TeamViewer активно используются хакерами для получения удаленного доступа, о чем стало известно еще в январе. Health-ISAC рекомендовала проверить журналы на наличие необычного трафика удалённого рабочего стола.

Хотя предупреждения от обеих компаний появились одновременно с сообщением TeamViewer об инциденте, не ясно, связаны ли они между собой. NCC Group и TeamViewer сообщили о взломе корпоративной среды, в то время как оповещение от Health-ISAC больше фокусируется на целевых атаках на подключения TeamViewer. Представители NCC Group и TeamViewer отказались предоставить дополнительные комментарии, заявив, что продолжают расследование инцидента.