ICANN73 | Виртуальный общественный форум — пленарное заседание: Эволюция диалога о злоупотреблениях DNS
Среда, 9 марта 2022 года, 10:30 – 12:00 по AST

БРЕНДА БРЮЭР: Можно начать запись?

Запись идет.

БРЕНДА БРЮЭР: Здравствуйте и добро пожаловать на пленарное заседание в рамках конференции ICANN73: Эволюция диалога о злоупотреблениях DNS

Меня зовут Бренда Брюэр (Brenda Brewer), на этом заседании я исполняю обязанности менеджера дистанционного участия. Пожалуйста, помните о том, что это заседание записывается, и придерживайтесь стандартов ожидаемого поведения ICANN. Для обеспечения транспарентности в рамках модели работы ICANN с участием многих заинтересованных сторон мы просим вас регистрироваться в конференциях Zoom с указанием полного имени. Например, имя и фамилия. Если вы войдете в это заседание, не указав свое полное имя, вы можете быть отключены.

Это заседание переводится на арабский, китайский, французский, русский и испанский языки. Нажмите кнопку «Перевод» на панели инструментов Zoom и выберите предпочтительный для вас язык.

Во время заседания опубликованные в чате вопросы и комментарии будут зачитываться только в том случае, если они соответствуют установленной форме, как я напишу в чате. Я буду зачитывать вопросы и комментарии в отведенное для этого время. Если во время той части заседания, которая будет посвящена дискуссии с сообществом, вы захотите высказаться, выберите на панели инструментов Zoom кнопку «Поднять руку».

Перед тем как говорить, отключите звук и уведомления на всех устройствах. Кроме того, не забудьте выбрать язык своего выступления. Пожалуйста, говорите четко и с нормальной скоростью, чтобы обеспечить точный перевод.

Когда ведущий заседания назовет ваше имя, включите свой микрофон и представьтесь для протокола. Чтобы вывести на экран стенограмму в реальном времени, нажмите кнопку

субтитров на панели инструментов Zoom. А теперь поприветствуем модератора Грэма Бантона (Graeme Bunton).

Прошу вас, начинайте.

ГРЭМ БАНТОН: Спасибо, Бренда. Всем доброе утро, день, вечер. Спасибо, что присоединились к нашему сегодняшнему пленарному заседанию, тема которого — эволюция диалога о злоупотреблениях DNS, злонамеренные регистрации и взлом доменных имен.
Меня зовут Грэм Бантон. Я директор Института по борьбе со злоупотреблением DNS.

Хочу сразу извиниться за объем того вступления, которое я сейчас вам представлю. У нас сложная тема, у нас замечательные участники дискуссии, но прежде чем мы перейдем к сути, нам нужно этому довольно основательно подготовиться. Пожалуйста, отнеситесь к этому с пониманием.

Наш первый участник дискуссии, Мацей, гораздо более основательно расскажет нам о сути этой темы. Я в остальной

части моего выступления просто хочу сделать так, чтобы мы все понимали, о чем речь.

Итак, сейчас я попытаюсь в двух предложениях рассказать вам о том, о чем мы будем сегодня говорить. Если говорить просто, наше сегодняшнее заседание посвящено изучению различий между мерами, применяемыми к доменам, которые были специально зарегистрированы для вредоносной деятельности, и доменами, которые также используются для вредоносной деятельности, но по той причине, что их веб-сайты были взломаны. То есть в одном случае кто-то намеренно пытался сделать что-то плохое с помощью доменного имени, в другом случае нет. И мы должны понимать, как эти сложные различия соотносятся с нашей экосистемой.

Итак, прежде чем мы погрузимся в суть этой проблемы, я хотел бы пройтись по некоторым моментам, касающимся целей этого заседания и круга вопросов, которые будут на нем рассматриваться, и в общих чертах рассказать вам о том, как мы, на мой взгляд, будем структурировать этот диалог.

Бренда, пожалуйста, покажите второй слайд.

Цели пленарного заседания, итак, это то, чего мы попробуем достичь за эти короткие 90 минут, которые у нас есть. Мы хотим попробовать выработать в сообществе понимание того, почему так важно разделять злонамеренные регистрации и взломанные сайты. Мы хотим поговорить немного о том, как нужно проводить это различие, но это в каких-то смыслах такая техническая проблема, поэтому мы не будем слишком в нее углубляться.

А углубляться мы хотим... и это самая суть этой дискуссии. Мы хотим выработать в сообществе понимание того, что может быть сделано в каждом из этих сценариев, злонамеренные регистрации и взломанные домены, и углубиться в эту проблему.

И затем, наконец, мы хотим поговорить о потенциальных действиях, о том, что мы можем сделать с этой проблемой, кто это должен делать, какова роль сообщества в этом.

Итак, давайте сейчас поговорим о круге вопросов. И это имеет важное значение. Я слишком долго работал с тематикой ICANN и принимал участие во множестве

пленарных заседаний. И я считаю, что существует зависимость между тем, насколько конкретно мы работаем с той или иной проблемой, и тем, сколько пользы нам удается извлечь из таких заседаний, как это. Так что я действительно хочу попросить всех сегодня вместе со мной оставаться в этих довольно узких рамках нашей темы.

В этой нашей дискуссии мы исходим из нескольких предположений. Мы на самом деле говорим сейчас о ситуации, в которой регистратура или регистратор получает сообщение о нарушении. Мы не будем сегодня обсуждать то, каким образом это сообщение поступает. Предположим, что факт нарушения подтвержден. То есть это действительно имеет место. Нам не нужно обсуждать, так это или нет. Такое подтверждение за рамками нашей темы.

И мы сегодня сосредоточим наше внимание в первую очередь на примерах вредоносного ПО и фишинга. Возможно, вы считаете, что злоупотребление DNS — это нечто другое. Наверное, нечто подобное лежит в основе представления о злоупотреблениях DNS большинства людей, но мы не будем сегодня дискутировать об определении. Позвольте мне выразиться предельно четко.

Мы не будем дискутировать об определении того, что собой представляет — или не представляет — злоупотребление DNS.

Мы на самом деле хотим понять это различие между злонамеренными регистрациями и взломанными сайтами.

Так что в течение всего нашего диалога мы будем действительно стараться держаться в рамках этой темы. Мы постараемся записывать те комментарии и вопросы, которые не относятся к этой теме, чтобы, возможно, вернуться к ним в будущем на каком-то более подходящем заседании.

Но я буду очень рьяно и энергично призывать нас придерживаться темы. Так что я прошу вас всех, когда вы будете подавать свои вопросы через функцию вебинара Q&A или обсуждать их в чате, придерживаться нашей темы и относиться с пониманием, когда я буду пытаться возвращать нас в ее рамки.

Следующий слайд, пожалуйста.

Итак, это что-то вроде карты нашей дискуссии, какой она будет сегодня. Итак, у нас есть сообщение о злоупотреблении DNS, которое поступило регистратору/регистратуре. Нам нужно поговорить немного о том, почему нам следует проводить это различие. Существует ли... должна ли это быть какая-то общего рода процедура рассмотрения сообщений о злоупотреблениях для всех видов нарушений? Если мы с этим не согласимся, если нам нужно проводить это различие, то нам нужно поговорить немного о том, каким образом проводится такое различие. Так сказать, по каким признакам регистрации мы можем относить ее к тому или иному роду?

И тут у нас есть два потока. У нас есть процедура, которую мы будем обсуждать, когда речь идет о злонамеренной регистрации доменных имен, то есть о тех доменах, которые специально регистрируются для нанесения вреда в Интернете. А другая процедура у нас будет для взломанных веб-сайтов, что мы должны делать в такой ситуации.

Небольшой спойлер — самая важная часть этой дискуссии, самая мякотка, так сказать, — это то, что мы как сообщество должны решить, какой должна быть процедура для

взломанных доменов. Но дальше мы рассмотрим более пристально обе эти ситуации.

И сегодня у нас замечательные участники дискуссии. Начнем мы со вступления, которое для нас проведет Мацей, профессор Университета Гренобля, (произносит по-французски) — так это, кажется, звучит по-французски, — который поделится с нами кое-какими фактами и поможет понять, что к чему. На это у нас будет приблизительно 15 минут.

А затем мы перейдем прямо к панельной дискуссии. А в панельной дискуссии у нас сегодня будут участвовать очень известные люди. Я хочу всех вас горячо поблагодарить за то. что присоединились к нам. С нами Лори Шульман (Lori Schulman) из группы интересов по вопросам интеллектуальной собственности (IPC). С нами Крис Льюис-Эванс (Chris Lewis-Evans) из рабочей группы GAC по обеспечению общественной безопасности, Алан Вудс (Alan Woods) от регистратур, Редж Леви (Reg Levy) от регистраторов и Род Расмуссен (Rod Rasmussen) от SSAC. Так что мы подробнее рассмотрим те темы, которые мы видим сейчас перед нами.

Они условно разбиты на два раздела. В одном мы ознакомим вас с вводной информацией, затем немного поговорим о злонамеренных регистрациях, а потом еще поговорим о взломанных доменах.

В конце мы отвели много времени для вопросов из аудитории. Я хочу сказать, что функция вебинара Q&A будет включена в течение всей этой дискуссии и я призываю вас пользоваться ею, с той лишь оговоркой, что мы должны оставаться в рамках той темы, которую мы будем рассматриваться сегодня.

Так что если ваш вопрос останется без ответа, мы его запишем для возможных дискуссий в будущем, но прошу вас не расстраиваться, если на него не ответят в контексте того, о чем мы будем говорить здесь сегодня.

Это, кажется, все, чем я хотел поделиться с вами в этом несколько затянувшемся вступлении, но я надеюсь, что у нас есть определенные ожидания, у нас есть четкие цели, определенный круг вопросов, так что, пожалуй, пора браться за дело.

На этом, я думаю, я готов передать слово Мацею, который расскажет нам о реальном положении дел на сегодня в том, что касается вредоносных регистраций и взломанных доменных имен.

Итак, Мацей, вам слово.

МАЦЕЙ КОРЧИНСКИЙ: Спасибо за вступление, Грэм.

Приветствую всех. Сегодня я кратко расскажу о проблеме различения между взломанными доменными именами и вредоносными регистрациями. Эта информация будет основана главным образом на проекте COMAR — это исследовательский проект, финансируемый AFNIC и SIDN, двумя операторами доменов .FR и .NL, а также на технической части исследования злоупотреблений DNS, проведенного по поручению Европейской комиссии.

Следующий, пожалуйста.

Итак, здесь вверху мы можем видеть URL-адрес, занесенный в черный список Phish Tank, а ниже вы можете видеть

вредоносный веб-сайт, снимок экрана такого веб-сайта. Итак, вопрос, на который мы пытаемся сегодня дать ответ — было ли данное доменное имя зарегистрировано для вредоносной деятельности. Следующий, пожалуйста.

Чтобы ответить на этот вопрос, нам нужно взглянуть на этот случай пристальнее. Итак, если мы перейдем по адресу зарегистрированного доменного имени, мы увидим, что там нет никакого осмысленного содержания, а если взглянуть на информацию в WHOIS, то мы увидим, что этот домен был зарегистрирован всего за два дня до внесения этого URL-адреса в черный список.

Следующий, пожалуйста.

То есть это довольно убедительно свидетельствует о том, что это доменное имя представляет собой случай вредоносной регистрации, злоупотребления с целью выдачи незаконного или запрещенного содержания, фишинга с целью хищения учетных данных и незаконного использования товарных знаков.

Итак, каковы будут последствия? Кто из посредников должен устранить это нарушение с технической точки зрения? Должен ли это быть оператор службы DNS, например, регистратор или регистратура TLD, наконец, или поставщик услуг хостинга. И почему это так важно? Потому что если мы приостановим только использование соответствующего доменного имени, а не вредоносного хостинга, тогда злоумышленник может просто зарегистрировать другое доменное имя и привязать его к вредоносному хостингу. С другой стороны, если мы заблокируем только хостинг, но не доменное имя, злоумышленник сможет использовать это доменное имя для осуществления других атак, в рамках других фишинговых кампаний.

Так что чтобы поставить более серьезные преграды для нарушителей и увеличить их экономические издержки, меры по устранению нарушения с технической точки зрения должны предусматривать реакцию как на уровне DNS, так и на уровне хостинга.

Следующий, пожалуйста.

Итак, давайте рассмотрим другой пример. Здесь у нас есть другое доменное имя... извините, другой URL-адрес, вредоносный URL-адрес, внесенный в черный список, если я правильно помню, антифишинговой рабочей группы. И ниже мы можем видеть снимок экрана с вредоносной страницей. Здесь тот же вопрос — было ли данное доменное имя зарегистрировано для вредоносной деятельности?

Следующий, пожалуйста.

И если мы перейдем по адресу этого зарегистрированного доменного имени, то там окажется веб-сайт з законным контентом, соответствующим доменному имени. Если мы посмотрим на информацию WHOIS, то это доменное имя было зарегистрировано еще в 2014 году, так что, скорее всего, само это доменное имя законное.

Кроме того, если взглянуть на вредоносный URL-адрес, то можно заметить строку wp-includes, указывающую на то, что настоящий веб-сайт был взломан с использованием уязвимости установленной системы WordPress.

Следующий, пожалуйста.

То есть это доменное имя законное, но веб-сайт подвергся взлому — злоупотреблению с целью выдачи незаконного или запрещенного содержания, фишинга с целью хищения учетных данных и незаконного использования товарных знаков.

Каковы будут последствия с технической точки зрения?

Обычно блокировать доменное имя должен не регистратор и не регистратура TLD, потому что это может нанести ущерб регистратору, его бизнесу, а также законным посетителям веб-сайта. Нарушения должны устраняться на уровне хостинга поставщиком услуг хостинга или же владельцем или администратором самого веб-сайта. При этом нужно сделать две вещи. Первое — удалить вредоносный контент, а также установить исправление уязвимости в системе WordPress на сайте.

А кто должен это сделать? Это должен быть поставщик услуг хостинга, если веб-сайт расположен, к примеру, на разделяемой платформе хостинга, где управление всем программным обеспечением, в т. ч. уязвимым, осуществляет

сама хостинговая платформа, или же, в случае неуправляемого хостинга, администратор веб-сайта, если уязвимое ПО находится в его управлении.

Следующий, пожалуйста.

Каким образом осуществляется злоупотребление законными доменами? По данным нашего анализа мы установили, что злоупотребления доменами обычно происходят на уровне веб-сайта. То есть злоумышленники могут воспользоваться уязвимостями в ПО, к примеру, в системе управления контентом. Иногда это происходит на уровне DNS. В качестве примера можно привести создание теневой копии веб-сайта, с помощью которой злоумышленники сначала пытаются похитить с помощью фишинга учетные данные регистраторов, владельцев доменов, чтобы получить доступ от их имени к панели регистрации. А войдя в панель регистрации, они могут, например, добавлять поддомены, которые могут использоваться, скажем, для фишинговых атак.
Следующий, пожалуйста.

Итак, какие существуют подходы к тому, чтобы различать законные, но захваченные доменные имена и доменные имена, которые были зарегистрированы с целью нанесения вреда?

Есть два подхода. Первый подход основан на эвристическом анализе и очень часто используется в отраслевых отчетах. Один из факторов эвристического анализа — возраст доменного имени. Как было показано, время с момента регистрации до внесения в черный список, шаблоны массовой регистрации, а также шаблоны в регистрируемых доменных именах. То есть, например, для фишинговых атак могут использоваться названия брендов или записанные с ошибками названия таких служб, как, к примеру, PayPal.

А вторая группа подходов основывается на методиках машинного обучения. Примером этого может служить система COMAR, разработанная в Университете Гренобль-Альпы и финансируемая AFNIC и SIDN. Это полностью автоматизированный подход, идея которого заключается в том, что мы собираем данные о хостинге веб-сайта, о структуре URL-адреса, определяем использование конкретных символов в доменных именах и т. д. и т. п., всего

мы извлекаем 38 таких атрибутов. Этот проект работает на основе полностью автоматизированной модели и демонстрирует точность до 97%.

Следующий, пожалуйста.
Есть ли какая-то зависимость между типом злоупотребления и взломанными доменными именами или злонамеренными регистрациями? Следующий, пожалуйста.

Здесь мы показываем распределение взломанных доменных имен (синим) и вредоносных регистраций (красным) по типам злоупотреблений. Для рассылки спама и управления ботнетами злоумышленникам, как правило, нужно контролировать DNS. Однако в случае фишинга и вредоносного ПО это не так. Атаки могут осуществляться с использованием как вредоносных регистраций доменных имен, так и взломанных веб-сайтов, а также бесплатных служб.

И, по нашим данным, около 25% доменных имен, используемых для фишинга, и 41% доменных имен, используемых для распространения вредоносного ПО, — это домены, которые были зарегистрированы законными

пользователями, однако затем были взломаны, скорее всего, на уровне веб-сайта.

Следующий, пожалуйста.

Итак, какова вариативность по разным типам доменов верхнего уровня? Итак, во второй половине 2021 года по новым gTLD мы наблюдали ситуацию, когда почти 98% доменов помечались как злонамеренная регистрация. Если посмотреть на национальные домены Евросоюза слева, то 42% доменов помечались как взломанные домены. А какие воз... какие возможные причины этого? Мы подозреваем, что в Европейском Союзе и в национальных доменах верхнего уровня (ccTLD) меньше спекулятивных регистраций, более функциональные веб-сайты с осмысленным содержанием, что означает также распространение различного потенциально уязвимого ПО, которое может использоваться киберпреступниками в массовом порядке.

Следующий, пожалуйста.

Здесь мы видим различия по разным доменам верхнего уровня.

Извините, кажется, у нас пропала связь. Я не вижу презентации.

ГРЭМ БАНТОН: Вы снова здесь, мы слышим вас, Мацей.

МАЦЕЙ КОРЧИНСКИЙ: Хорошо. Но я не вижу презентации.

ГРЭМ БАНТОН: Сейчас на экране слайд 13.

МАЦЕЙ КОРЧИНСКИЙ: Да, хорошо. Я просто переключусь... на локальную версию у себя. Хорошо.

Итак, здесь мы можем видеть общее количество доменных имен, количество доменов с нарушениями по разным доменам верхнего уровня, а также количество доменов, зарегистрированных со злым умыслом, количество взломанных и, в частности, в последнем столбце мы можем видеть долю злонамеренных регистраций в общем числе

доменов в нарушениями по каждому домену верхнего уровня. Следующий, пожалуйста.

Итак, здесь мы видим, что по некоторым доменам верхнего уровня доля злонамеренной регистрации доменных имен составляет почти 100%.

Только нужно сказать, что доменные имена в зонах .TK и .ML — это домены, которые Freenom раздает своим пользователям бесплатно, а это привлекательная лазейка для, скажем, фишинга.

Следующий, пожалуйста.

С другой стороны мы также видим домены верхнего уровня с. К примеру, в зоне .BR злонамеренная регистрация доменных имен составляет всего 34%. И на это может влиять множество факторов. Я попрошу вас обратить ваше внимание на то, что к этим результатам нужно относиться с осторожностью ввиду ограничений классификаторов, а также ввиду ограничений самих этих черных списков. Они могут быть не отражать картины во всем киберпространстве.

Почему? Потому что некоторые составители черных списков могут фокусировать свое внимание на случаях злонамеренной регистрации доменных имен, используя для этого... определенные ключевые слова и т. п.

И еще один момент, который я также хотел бы здесь упомянуть, — то, что мы видим в черном списке, может отличаться от того, что получают службы поддержки регистратур доменов верхнего уровня, когда они еще раз анализируют жалобы жертв атак, потому что такие черные списки могут быть недостаточно репрезентативными.

И мое последнее замечание: время от времени мы видим довольно большую вариативность по одному и тому же домену верхнего уровня, например, .INFO или .COM, в разные месяцы. Что может быть причиной? Одной из возможных причин может быть то, что какой-то реселлер, к примеру, предоставляет большие скидки на доменные имена, которые используют злоумышленники. И в таком случае мы видим увеличение доли злонамеренной регистрации доменных имен в общем количестве доменов, используемых для осуществления вредоносной деятельности. Или же, к примеру, время от времени мы видим, что обнаруживаются

какие-то уязвимости, например, в системах управления контентом, и это затрагивает сотни тысяч доменных имен. А это тоже легкая добыча для злоумышленников. Они могут массово их использовать. И тогда, в таком случае, в течение непродолжительного времени мы видим сокращение доли злонамеренной регистрации доменных имен в общем количестве доменов.

Следующий, пожалуйста.

Итак, большое спасибо за внимание. Надеюсь, это поможет нам начать дискуссию. Спасибо.

ГРЭМ БАНТОН: Спасибо, Мацей. В своем рассказе вы ответили на ряд вопросов, которые поступали, так что спасибо вам за это.

Но там еще немного было в чате, Мацей, спрашивают, а можно ли это делать с помощью машинного обучения? Существуют ли какие-то алгоритмы обнаружения, и какова их точность? И я не думаю, что нам нужно слишком углубляться в то, как именно это можно сделать, но мне кажется, будет полезно, если вы выделите нам две-три

минуты и расскажете о различных атрибутах самих доменных имен или связанных с ними веб-сайтов, а также о том, как можно попытаться сделать это с помощью каких-то инструментов автоматизации, так сказать, какие инструменты для этого могут использовать люди, у которых нет таких технологий. Не могли бы вы для меня это сделать?

МАЦЕЙ КОРЧИНСКИЙ: Конечно. Итак, по первому вопросу, мы действительно проводили анализ важности различных функций классификатора COMAR.

То есть классификатор COMAR, как уже было сказано в ходе презентации, — это полностью автоматизированный алгоритм машинного обучения. Его очень полезные функции основаны на работе с контентом. То есть, к примеру, если мы обнаруживаем, что для создания того или иного веб-сайта использовалось множество различных технологий, это указывает на то, что этот веб-сайт был взломан.

Если мы видим определенные положительные ключевые слова, такие как PayPal, но не просто названия брендов, а

очень специфические ключевые слова, это как верификация, мы также проводили анализ ключевых слов. Тогда это указывает на злонамеренную регистрацию такого веб-сайта.

А классификатор может анализировать и определять какие-то признаки, такие как количество используемых технологий, что для человека было бы гораздо сложнее.

С другой стороны, если нам нужно будет сделать это вручную, то есть несколько признаков, которые мы видели в примерах, скажем, время, прошедшее с момента регистрации до внесения в черный список. Если это очень короткое время, то это с большой степенью вероятности указывает на то... на злонамеренную регистрацию самого этого доменного имени.

Если мы видим, что на сайте по зарегистрированному доменному имени нет осмысленного содержания, или же, скажем, по зарегистрированному доменному имени расположен настоящий фишинговый веб-сайт, то это тоже указывает на злонамеренную регистрацию такого доменного имени.

И эти два примера — это хорошие примеры того, как такие вещи могут определяться как людьми, так и нашими алгоритмами на основе машинного обучения.

ГРЭМ БАНТОН: Прекрасно. Спасибо, Мацей. Тут еще много всякого в чате. Я не могу уследить за чатом, потому что там слишком много всего. Так что если у вас есть вопрос, на который вы хотели бы получить ответ и который, опять же, по этой теме, воспользуйтесь функцией вебинара Q&A, чтобы мы могли его записать.

Итак, есть ряд вопросов о том, как работает это обнаружение. Из того, на что вы можете взглянуть, недавно в DNSAI выпустили документ о передовых практических методиках в этой области.

Я уверен, что кто-то из моих друзей может найти ссылку и опубликовать ее в чате. Прошу вас, и спасибо.

И я также сам подготовил в понедельник, в рамках Tech Day, презентацию по архитектуре такого рода решений, в

которой, как мне кажется, представлена некая концепция того, как это может делаться.

Но мне кажется, что нам нужно уходить от того, как это делается. Очевидно, что есть большой интерес к этой технологии или к человеческому подходу к вынесению таких решений о том, является ли та или иная регистрация злонамеренной. Но, мне кажется, нам нужно переходить к тому, почему и что делается.

И это будет мой первый вопрос к участникам дискуссии. Участникам дискуссии подготовиться.

Это такой вопрос, от которого зависит все остальное: Следует ли нам вообще этим заниматься? Имеет ли смысл двоить наши процессы борьбы с нарушениями? Следует ли нам различать злонамеренные регистрации и взломанные домены, или же нет? Так сказать, следует ли нам использовать один и тот же подход для всего, такой общий подход к злоупотреблениям, или же нам следует использовать для этого разные процедуры?

Так что мне интересно, есть ли для начала кто-то, кто не согласен с этой посылкой. Следует ли нам одинаково относиться ко всем злоупотреблениям?

Так что давайте с этого начнем и посмотрим, не хочет ли кто-то из наших участников дискуссии вкратце высказаться по этому вопросу.

Я вас выберу. Редж, прошу вас.

РЕДЖ ЛЕВИ: Разумеется. Да. Я считаю, что проводить такое различие совершенно необходимо. У нас есть много клиентов, использующих коммерческие инструменты для создания веб-сайтов, которые необходимо регулярно обновлять. И если эти обновления не выполнять, то такие инструменты часто становятся уязвимыми для взлома. То есть нужно связываться с владельцами доменов и обсуждать с ними то, что они должны сделать что-то, что они не сделали десять лет назад, с доменом, о котором они, возможно, уже пять лет не вспоминали с тех пор, как запустили в работу этот веб-сайт. И они просто используют электронную почту и считают, что можно зайти на веб-сайт, посмотреть

информацию и связаться с ними, и такова процедура. И мы должны сделать так, чтобы их бизнес не пострадал из-за того, что их домен был взломан.

ГРЭМ БАНТОН: Спасибо, Редж.

Сейчас выступает Алан, затем Крис, а потом Лори. И мне кажется, что нам не нужно слишком углубляться в «почему». Посмотрим. А затем мы потихоньку пойдем дальше.

Алан, прошу вас.

АЛАН ВУДС: Большое спасибо. Алан Вудс (Alan Woods), для протокола.

Итак, да, я считаю, что важно проводить это различие. И я знаю, что это та причина, которая выдвигается постоянно уже очень много лет. Но с точки зрения нас как оператора регистратуры, когда мы принимаем меры в отношении домена, это приводит к множеству неприятных побочных последствий. Поэтому мы не хотим обвинять в чем-то того,

кто сам является жертвой, как в данном случае, когда владелец домена является жертвой взлома.

Так что я считаю, что нам нужно очень четко сказать, что если мы будем принимать меры, то мы должны иметь представление и понимание об этом различии. Я хотел сказать «о нюансе», но это различие, которое существует также между этими двумя видами жертв.

ГРЭМ БАНТОН: Да. Спасибо, Алан.

Крис.

КРИС ЛЬЮИС-ЭВАНС: для протокола. Да, спасибо, Грэм. Это Крис Льюис-Эванс (Chris Lewis-Evans),

Я только хочу здесь согласиться, я считаю, что мы должны по-разному к этому относиться. Как сказал Алан, у нас здесь есть два разных вида причиняемого вреда. То есть в случае злонамеренной регистрации домена у нас есть основной

вред. А в случае взломанного домена у нас есть основной вред, но помимо это есть еще побочный вред.

То есть в случае взломанного домена у нас есть два типа жертв: основная жертва, а также те, кто мог подвергнуться побочным вредным последствиям. То есть на самом деле мы должны иметь возможность работать и с теми, и с другими, и оказывать достаточную помощь и тем, и другим.

ГРЭМ БАНТОН: Спасибо, Крис.

Лори, прошу вас.

ЛОРИ ШУЛЬМАН: Да. Я хотела сказать, что группа интересов по вопросам интеллектуальной собственности согласна с тем, что их совершенно необходимо различать. Нужно различать между злонамеренными и взломанными доменами, по меньшей мере в том, что касается скорости нашего реагирования в том или ином случае.

Однако в то же время я бы не хотела, чтобы мы в этой проблеме потеряли из виду то, кто на самом деле является жертвой, потому что есть конечный пользователь, и именно на конечного пользователя направлена атака с использованием фишинга или вредоносного ПО.

Однако также, особенно в случае малого бизнеса, потенциальной жертвой является также владелец этого взломанного домена, потому что это вредит его репутации. И я не думаю, что мы должны исходить из предположения о том, что владелец домена, который ведет свой бизнес или... или занимается каким-то... это не обязательно должен быть бизнес, это может быть какая-то организация, представленная на этом веб-сайте, что он не предпочел бы, чтобы его сайт был какое-то время недоступен, если речь идет на самом деле о защите клиентов или своей репутации.

ГРЭМ БАНТОН: Спасибо, Лори.

Итак, из того, что я понял, получается, что все, по крайней мере в этой группе, согласны с этим вопросом, с тем, что нам

следует на самом деле проводить это различие. И это замечательно.

Но это также усложняет нам жизнь. Так что сейчас нам нужно начать немного углубляться в то, что это означает. При этом через функцию вебинара Q&A нам пришло множество вопросов, на которые, мне кажется, нам следует попытаться ответить, пока они актуальны, прежде чем мы пойдем дальше. Я могу попробовать выбрать некоторые из них и назначить их участникам дискуссии. И мы попробуем так сделать.

Был вопрос от Грега Шатана (Greg Shatan), на который, как мне кажется, ответит Мацей. Итак, он спрашивал: Какое место в вашем подходе отводится злоупотреблениям на уровне почтового сервера?

Мне кажется, что злоупотребления на уровне почтового сервера — это довольно интересно. Я недостаточно об этом знаю.

Мацей, у вас есть какие-то мысли в отношении того, как к этому подходить?

МАЦЕЙ КОРЧИНСКИЙ: Почтовый сервер?

ГРЭМ БАНТОН: То есть мне кажется, что Грег спрашивает о ситуации, когда фишинг или распространение вредоносного ПО осуществляется через электронную почту.

МАЦЕЙ КОРЧИНСКИЙ: Можно, чтобы это вопрос задал его автор?

Возможно, так будет проще его прояснить.

ГРЭМ БАНТОН: Я не совсем уверен, что будет удобно включать голос сейчас таким образом.

Возможно, Грег сможет уточнить это в чате, а мы вернемся к этому позже.

МАЦЕЙ КОРЧИНСКИЙ: Спасибо.

ГРЭМ БАНТОН: И посмотрим, возможно, он уточнит.

МАЦЕЙ КОРЧИНСКИЙ: Огромное спасибо.

ГРЭМ БАНТОН: На что еще мы можем попробовать ответить, прежде чем мы уйдем далеко вперед. Ого, здесь много. Пожалуйста, подождите немного, пока я не выберу что-то, что подходит.

Еще один вопрос к Мацею от Самане. Она интересуется, эта методика машинного обучения и эта функция, которая используется в системе COMAR, включает ли она те эвристические алгоритмы, которые вы упомянули, когда говорили о первом методе. Если да, то какие примеры можно привести?

МАЦЕЙ КОРЧИНСКИЙ: Благодарю за вопрос. Да, то есть мы включили в эти методы почти все функции, которые используются в эвристическом анализе, кроме массовой регистрации. Это единственная функция, которую мы не включили. А причина... я бы сказал, что есть две причины. Одна причина — это то, что мы...

основная причина — это просто то, что методика COMAR должна различать между злонамеренной регистрацией и взломанными доменами только на основе собранных данных применительно к одному конкретному случаю, без... не извлекая информацию, к примеру, из других злонамеренно зарегистрированных доменных имен.

Но помимо этой одной функции в полностью автоматизированной системе COMAR реализованы все алгоритмы эвристического анализа.

ГРЭМ БАНТОН: Спасибо, Мацей.

Кажется, здесь есть еще один вопрос для вас от Майкла Пеледжа (Michael Palage), его интересует ваше мнение о большой доле взломанных доменных имен в европейских национальных доменах ccTLD, и не... не объясняется ли это, возможно, тем, что все больше доменов ccTLD выполняют идентификацию личности? Злоумышленникам проще взломать домен/веб-сайт или же зарегистрировать доменное имя с поддельными или синтезированными данными владельца?

МАЦЕЙ КОРЧИНСКИЙ: Если я правильно понял этот вопрос — почему мы видим меньше злонамеренных регистраций и больше взломанных веб-сайтов в национальных доменах ccTLD Европейского Союза. Так?

Ответ я уже пытался немного обсуждать в ходе презентации. Но мы можем только строить рассуждения, потому что измерений мы никаких не проводили.

Но я бы сказал, что в доменах ccTLD Европейского Союза у нас, как уже было сказано... как уже было сказано, много... меньше запаркованных доменов, не так много спекулятивных доменов. За этими доменными именами есть веб-сайты. А если там есть веб-сайты, то кто-то ими занимается. Они устанавливают... развертывают разное программное обеспечение. И поскольку мы видим на веб-сайте множество различных программ, некоторые из этих программ могут просто... могут быть просто... могут содержать уязвимости, которые будут использованы злоумышленниками.

И, кажется, вторая часть вопроса была о том, почему мы видим меньше злонамеренных регистраций доменных имен. Это также просто предположение. Но в доменах ccTLD реализовано множество инициатив, направленных на недопущение злонамеренных регистраций. Скажу только, что в ccTLD .eu есть система, аналогичная системе Premadoma, которая определяет домены... злонамеренную регистрацию доменов во время регистрации. Есть и другие операторы ccTLD, которые активно борются и пытаются предотвращать такую злонамеренную регистрацию, как это делают, например, SIDN и AFNIC.

Но это я больше говорю из моего опыта, а также из результатов исследований и практики работы, которые я наблюдают в доменах ccTLD. Это не значит, что, к примеру, другие национальные домены ccTLD или другие группы доменов ccTLD не используют такие методы.

ГРЭМ БАНТОН: Спасибо, Мацей.

Итак, тут у нас много вопросов и много чего происходит в чате. Мы постараемся не утонуть в этом всем.

Участники дискуссии, если вы хотите ответить на вопрос, вживую или через функцию вебинара Q&A, прошу вас.

Однако я думаю, может на этом нам следует немного двигаться к этой левой части этой диаграммы и начать говорить о том, как мог бы выглядеть процесс борьбы со злонамеренными регистрациями и какие тут могут быть соображения. Просто хочу еще раз уточнить, сверить часы, так сказать, — мы решили, что следует различать. Мы немного поговорили о том, как мы можем принимать такое решение. То есть у доменного имени есть какие-то атрибуты. Может, это будет система на основе машинного обучения. Возможно, это будет делать живой человек. Теперь нам нужно придумать, что мы будем делать.

То есть на уровне регистратур и регистраторов, там не так много вариантов, но, пожалуй, нам следует немного их рассмотреть.

И на этот раз я передам слово Роду. Род, если у вас есть какие-то мысли в отношении того, какие действия должны предпринимать регистратуры или регистраторы,

сталкиваясь со злоупотреблениями DNS, когда они считают, что имеет место злонамеренная регистрация.

У вас есть какие-то идеи по этому поводу?

РОД РАСМУССЕН: Да, спасибо. Это Род Расмуссен (Rod Rasmussen).

Итак, после того как вы определили... приняли решение с использованием той или иной методики, и мы пока отложим этот вопрос и не будем на нем фокусироваться. Мы говорим, мол, хорошо, мы приняли решение о том, что это злонамеренная регистрация, что я могу сделать?

И у нас есть... если вы регистратор/регистратура, то у вас на самом деле совсем мало вариантов. То, что мы можем сделать, сводится практически к одному — удалить сам домен из глобальной DNS.

И это на самом деле можно сделать несколькими способами. Его можно прямо вот взять и удалить, и так и сказать, что мы эту регистрацию удаляем. Если у вас есть злонамеренная регистрация, оформленная, так сказать, в последние пару дней, вы на самом деле можете... воспользоваться

возможностью получить за это какую-то финансовую компенсацию. Иными словами, вам вернут деньги. То есть в этом преимущество, а недостаток этого в том, что то, кто изначально этот домен зарегистрировал, может просто снова его зарегистрировать, через того же регистратора или где-то еще, просто снова использовать ту же схему, какой бы она ни была, даже если вы... даже если в то же время вредоносный контент будет где-то устраняться, где бы он ни был, но злоумышленники, конечно же... знаете, у них есть много взломанных веб-сайтов, на которых они могут пробовать провернуть то же самое. Это такие преимущества и недостатки.

Можно приостановить работу домена. Иными словами, вы его не удаляете, а просто переводите в категорию приостановленных. Оно будет удалено из DNS, но продолжит существовать где-то в статусе приостановленного до завершения срока регистрации. И тогда вам, если вы регистратор, или регистратура, или и то, и другое, вам придется этим заниматься.

Еще вы можете... есть и другие меры активной борьбы, к которым вы можете прибегнуть. В течение многих лет

антифишинговая рабочая группа поддерживает специальную страницу для фишинговых сайтов, то есть вы можете на самом деле перенаправлять туда... при фишинговых атаках, например, вы можете перенаправлять... вы можете на самом деле внести в DNS такие изменения, чтобы этот домен указывал на эту специальную антифишинговую страницу. Что-то подобное делали и другие. Если это что-то вроде вредоносного ПО, вы можете создать т. н. воронку, что даст вам возможность информировать пользователей о том, что их компьютер был взломан. Это многими разными способами не раз делали либо непосредственно провайдеры, либо же компании, специализирующиеся в области безопасности, правоохранительные органы и т. п. То есть вы можете на самом деле активно пытаться информировать жертв вредоносного ПО о заражении их компьютеров. Для этого вам может понадобиться перевести доменное имя другой организации, с точки зрения регистратуры... регистратора... извините, владельца домена. То есть, например, ФБР брало под свой контроль какие-то домены и переводило их в другие организации. Корпорация Microsoft тоже не раз это делала.

Вы также можете... есть... можно использовать т. н. регистратора последней инстанции, который специально создан для передачи ему доменов, с которых осуществляется управление вредоносным ПО, чтобы потом автоматически возвращать эти данные жертвам. То есть здесь есть несколько разных вариантов, но это действительно подразумевает определенную работу, чтобы у вас была какая-то процедура и документально оформленные юридические основания.

И последнее, что я хотел бы добавить к этому, это то, что после того, как вы определите, что у вас имела место злонамеренная регистрация, будет очень разумно проверить, нет ли других доменов, которые регистрировались подряд или используются потенциально одним и тем же владельцем или учетной записью владельца. Нужно проанализировать такую учетную запись, потому что важно — я думаю, Редж или кто-то еще сможет подробнее об этом рассказать — понять, была ли эта учетная запись создана злоумышленниками или же взломана для добавления в нее таких доменов, потому что ее владелец может сам быть жертвой фишинга или какого-то хищения учетных данных.

А еще нужно смотреть, нет ли какого-то шаблона, массовой регистрации учетных записей, возможно, под разными псевдонимами и т. п., чтобы иметь возможность обнаруживать злоупотребления по широкому ряду доменов и, возможно, учетных записей владельцев, которые могут... обычно они используются для поддержки масштабных кампаний, потому что многие из этих злоумышленников очень грамотно скрываются от добросовестных регистраторов, которые пытаются не допускать их в свои системы.

Это такие соображения вашему вниманию.

ГРЭМ БАНТОН: Спасибо, Род. Отличное выступление. И очень содержательное.

Если позволите, я кратко суммирую: у регистраторов есть три или... у регистраторов больше, чем у регистратур, хотя регистратуры тоже могут в этом участвовать, но домены можно удалять, что, наверное, не очень хорошо, их можно приостанавливать, а можно перенаправлять. И для всех этих

трех мер должны быть основания. А затем может быть полезно проверить учетную запись, проверить, не отвечает ли она какому-то отдельному шаблону. На мой взгляд, все это очень полезная информация для тех, кто занимается борьбой со злоупотреблениями.

Мне интересно, как это видят Редж или Алан из наших участников дискуссии. Часто ли они используют эти методы? Если да, то почему? Почему нет?

Но прежде чем... пока вы это обдумываете, Лори, вам слово.

ЛОРИ ШУЛЬМАН: Спасибо. У меня вопрос к тому, что Род сказал о шаблонах злоупотреблений и о том, чтобы искать более широкие... более широкие наборы примеров. В сегодняшних условиях, с учетом тех ограничений, которые на нас возложены законодательством и текущими политиками, ограничиваются ли такие исследования только доменами одного конкретного регистратора или же регистраторы могут анализировать данные других регистраторов, тогда, может, имело бы смысл, чтобы это делали не регистраторы, а регистратуры?

ГРЭМ БАНТОН: Да, так можно. Спасибо, Лори.

Род?

РОД РАСМУССЕН: Да, давайте я отвечу. Ответ да на оба вопроса (смеется). Это... и... у регистратора есть уникальная возможность видеть то, что было скрыто от широкой публики, когда речь идет о контактных данных и т. п., и это важное преимущество, очень важное преимущество в этом деле, в проведении такого рода эвристического анализа и т. п., о котором перед этим говорил Мацей. Но... и у них есть возможность видеть, откуда регистрировались владельцы, какие кредитные карты они использовали, такого рода данные. То есть у них гораздо больше внутренних данных, которые можно анализировать.

Регистратура же со стороны может очень хорошо видеть шаблоны действий, особенно если она поддерживает обнаружение т. н. алгоритмов создания доменных имен. Они используются вредоносным ПО, которое регистрирует

заранее определенный набор доменов, чтобы осуществлять управление семействами вредоносных программ. Когда вы видите серию таких регистраций у разных регистраторов, вы понимаете, что это делается по шаблону.

Они могут также анализировать такие вещи, как хостинг DNS и настройки соответствующих доменов в Интернете. То есть если взглянуть на то, как они настраиваются для использования конкретных серверов DNS, серверов имен или IP-адресов конечного хостинга, можно... зачастую можно обнаруживать такого рода вещи, или по меньшей мере замечать подозрительные тенденции. Это то, что затем можно проанализировать глубже и попросить регистраторов сделать это, проанализировать эти учетные записи и проверить, не занимаются ли они чем-то нехорошим.

ГРЭМ БАНТОН: Спасибо, Род.

Только одна мысль, пожалуй, для Криса. Если вы... это не обязательно... я дам слово Редж и Алану, прежде чем вернусь к вам, но прежде чем мы уйдет от этой темы и взломанных

доменов, мне интересно, с точки зрения правоохранительных органов, когда речь идет о злонамеренной регистрации, вас больше устраивает просто остановка их работы или же... или же вы часто расследуете злонамеренные регистрации, чтобы получить из этого больше информации.

Но сейчас кратко Редж и Алан. А затем, возможно, Крис. Затем, пожалуй, мы попробуем перейти к взломанным доменам, после чего еще поотвечаем на вопросы.

Редж.

РЕДЖ ЛЕВИ: Спасибо, Грэм. Это Редж Леви из Tucows. Мы оптовый регистратор, то есть наш подход к этому будет немного отличаться от подхода регистратора, который непосредственно взаимодействует с владельцами доменов.

Мы работаем в основном с нашими реселлерами и ищем шаблоны по реселлерам. То есть когда начинает поступать много сообщений о злоупотреблениях по конкретному реселлеру, мы обращаемся к нему и заявляем, мол, мы

специалисты по борьбе со злоупотреблениями DNS. Как мы можем вам помочь? И обычно мы на этой основе решаем проблемы.

При этом у нас также есть свой собственный реселлер, и когда мы видим наплыв злонамеренных регистраций по нашему реселлеру, мы можем принимать меры непосредственно против владельцев соответствующих доменов, если удается установить, кто они.

И, как уже было сказано в чате, зачастую злоумышленники не используют правильные... настоящие имена или одни и те же имена для регистрации множества доменов. То есть поиск такого рода шаблонов не всегда помогает.

Хотя, я думаю, первоначальный вопрос был в том, отслеживаем ли мы их при регистрации доменов, чтобы принимать решение о том, является ли данный домен злонамеренным или взломанным? Да, конечно, мы это делаем. К сожалению, очень часто искусственный интеллект, и об этом также говорилось в чате, пропускает какие-то вещи или дает... слишком широкий спектр оценки, чтобы можно было принимать решения об остановке работы домена. То

есть то, что мы получаем от искусственного интеллекта, нам потом еще нужно тщательно проверять вручную.

Одна из моих любимых историй на самом деле касается алгоритма генерирования доменов. Какой-то бедняга умудрился зарегистрировать строку, в точности совпадающую с набором случайных символов, выданных алгоритмом создания доменных имен, но это была настоящая аббревиатура названия небольшой женской футбольный команды из... я точно не помню, где-то в Центральной Америке. Так что (смеется) мы связались с правоохранительными органами и регистратурой, чтобы позволить им на самом деле зарегистрировать этот домен.

Но это, опять же, пример того, как такого рода компьютерные алгоритмы слишком широко определяют потенциальные проблемы. Извините.

ГРЭМ БАНТОН: Спасибо, Редж. Милая история.

Алан, затем Крис. Если можно, кратко, пожалуйста, чтобы мы могли двигаться дальше. Спасибо.

АЛАН ВУДС: Разумеется. Пожалуй, в двух словах. Обращаться к регистратору — это замечательно, потому что именно так регистратура и должна действовать в этом диалоге. Я все то же самое, что говорила Редж, но на более высоком уровне. Там, где она связывается со своими реселлерами или своими владельцами доменов, для меня первый, с кем я связываюсь — это мой регистратор. И я считаю, что это очень важно, чтобы с точки зрения регистратуры, когда я оказываюсь в такой ситуации, да, сначала мы смотрим на эти индикаторы, в чем-то это делает для нас наша технологическая платформа TDNS, но главное — это доказательства, с которыми можно уже обращаться к моим регистраторам, чтобы они уже гораздо более конкретно разговаривали со своими владельцами доменов.

И мне кажется, что мы сейчас сбились на разговор об обнаружении, от которого я хотел бы уйти, потому что мы говорим здесь о взломанных доменах и о том... что нам делать и как обнаруживать такие взломы. То есть мне кажется, что это важный аспект этого.

И я хочу сказать еще одно, что мне кажется также важным с точки зрения регистратуры. Я хотел бы немного вернуться к тому, о чем говорила Лори, кажется, что предприятия малого бизнеса предпочли бы или не возражали бы, если бы их бизнес остановился. Я думаю, многие предприятия малого бизнеса категорически с вами бы не согласились в этом. Я считаю, что нам нужно четко понимать, что все дело в соотношении ущерба. Кому больше наносится ущерб, владельцу домена или конечному пользователю? Если можно, давайте исходить из этого базового понятия соотношения, вместо того чтобы делать какие-то глобальные широкие заявления, я думаю, что дело несомненно в соотношении ущерба, и нам нужно это обсудить.

ГРЭМ БАНТОН: Спасибо, Алан. И это будет замечательным вступлением к следующей части нашей дискуссии, я вернусь к этому балансу ущерба через минуту, а пока послушаем Криса.

КРИС ЛЬЮИС-ЭВАНС: Да, спасибо. Это Крис Льюис-Эванс, для протокола.

Итак, если говорить о злонамеренной регистрации доменов, потому что, Грэм, ваш вопрос ко мне, на мой взгляд, об этом, — да, в конечном итоге мы здесь говорим о вредоносном ПО и фишинге, так что обычно какое-то расследование в таких случаях проводится в той или иной форме. И вряд ли это кого-то удивит, но обычно они регистрируют не один домен.

Так что... в отношении этого домена будет проведено расследование, а также какая-то работа, которую мы можем провести с регистратурами, регистраторами или поставщиками услуг хостинга, чтобы обнаружить другие домены, чтобы не реагировать по факту, а работать на опережение, потому что в таких случаях всегда будут еще жертвы и еще ущерб. Так что да, конечно же, правоохранительные органы всегда стараются именно так и поступать, работать на опережение, чтобы предотвратить нанесение ущерба.

Спасибо.

ГРЭМ БАНТОН: Спасибо, Крис.

Хорошо. Итак, у нас осталось примерно 35 минут, нам нужно еще успеть ответить на множество вопросов в очереди, и в чате тоже много чего происходит. Пока же большое вам всем спасибо за то участие, которое мы наблюдаем. Но мне кажется, что пока мы делали легкую работу, то есть мы выяснили, что нам нужно проводить это различие. Мы немного поговорили о том, как это делать. Мы немного поговорили о той замечательной информации, которую нам дал Род о том, что нужно делать в случае злонамеренной регистрации . А сейчас у нас другая сторона, которая, на мой взгляд, сложнее, это ситуации злоупотребления DNS, в которых через взломанные веб-сайты распространяется вредоносное ПО и осуществляется фишинг. То есть сам веб-сайт ничего плохого не делает. Это может быть небольшая компания или чей-то блог. Он на самом деле не... ну, или делает, и это то, о чем мы и поговорим.

Как при таких обстоятельствах нужно выяснять, что следует делать? Как оценить баланс ущерба, как это обычно делается?

Так что я, пожалуй, начну с такого немного провокационного вопроса снова к Редж и Алану, а именно: если вы выяснили,

что тот или иной сайт взломан и через него осуществляется фишинг или распространяется вредоносное ПО, имеет место злоупотребление DNS, существуют ли какие-то обстоятельства, при которых вы его закроете? Скажем, приостановите домен, по которому расположен взломанный веб-сайт.

Алан?

АЛАН ВУДС: Спасибо. Тут как по волшебству вопрос снова о соотношении ущерба. То есть это интересный вопрос, и я считаю, что мы как регистратура должны четко понимать, что те инструменты, которые в нашем распоряжении, очень грубые, то есть это приведет к недоступности всего, что было на этом веб-сайте, всего, что было на этом домене, любой электронной почты, которая была на этом домене. То есть чтобы регистратура на самом деле сказала: знаете что? В данном случае мы не получили ответа от регистратора, мы не получили ответа от владельца домена, а ущерб, который объективно значителен, по-прежнему наносится. Да, я хочу сказать, что всегда может быть ситуация, в которой мы захотим его закрыть, но вопрос в соотношении ущерба. Идет

ли речь... извините, я буду говорить медленнее для переводчиков. Я увлекся.

Мы говорим, так сказать, о вещах, которые наносят ущерб людям в их жизни. Мы имеем в виду такие вещи, как материалы, связанные с сексуальной эксплуатацией детей, это чрезвычайно, чрезвычайно ужасные вещи. И мы должны четко заявить, что по возможности закрывать и блокировать должна не регистратура, но в тех случаях, когда это необходимо, у нас есть такая возможность.

ГРЭМ БАНТОН: Спасибо, Алан.

РЕДЖ ЛЕВИ: И в продолжение...

ГРЭМ БАНТОН: Прошу вас, Редж.

РЕДЖ ЛЕВИ: В продолжение этого, мы тоже стараемся использовать приостановку взломанных доменов только как крайнюю меру. Мы связываемся с реселлером и непосредственно с

владельцем домена и говорим, мол, что-то происходит. Можете решить эту проблему? И мы можем, исходя из их ответа или его отсутствия, начать сбрасывать разные записи одну за другой, то есть мы можем выключить почту, мы можем... если взлом или заражение осуществляется таким образом. Мы можем сбросить сервер имен, если взлом осуществляется через него.

Иногда в таких случаях люди отвечают и говорят, мол, знаете, мы не знали, что на это ваше письмо нужно было ответить, не могли бы вы включить мой (неразборчиво), и тогда я все исправлю. И это еще один аспект этого, то, что иногда домен... нам нужно обеспечить разрешение доменного имени, чтобы владелец мог войти на свой сайт и устранить проблему.

Так что приостановка домена позволит остановить злонамеренное использование, но зато не позволит делать ничего другого и не даст возможности устранить злоупотребление.

ГРЭМ БАНТОН: Большое спасибо за эту информацию, Редж и Алан.

Мне интересно, Лори, Род, Крис, есть какая-то информация, которую, на ваш взгляд, нужно учитывать при определении соотношения ущерба, чем часто приходится заниматься регистраторам, какая-то информация, которая, возможно, в недостаточной степени учитывается или может быть... или которой, возможно, следует придавать большее значение при определении того, как следует поступить в отношении взломанного веб-сайта, через который осуществляется злоупотребление DNS.

ЛОРИ ШУЛЬМАН: Да, Грэм, я, если вы не против, первой отвечу на этот вопрос, учитывая то, что обсуждается в чате. Потому что я в чате сказала то, что решительно оживило дискуссию. Но это касается того, что объясняет Редж и с чем я согласна, что когда вы ищете взломанные домены, вы не обязательно имеете дело с фактами. Это именно то, что я пыталась сказать в чате, но, кажется, это было немного не так интерпретировано, да?

Когда вы анализируете взломанные доменные имена, вы находитесь в совершенно иной ситуации принятия решения

о том, что вам делать, когда это делать, как это делать, потому что это касается... возможно, (неразборчиво), это работающий веб-сайт, который предлагает какую-то услугу или еще какие-то полезные вещи, и если мы приостановим работу этого домена, то этих полезных вещей не станет. Это может касаться чьего-то дохода. Это хорошее замечание.

Но я пытаюсь сказать следующее: в зависимости... и это касается также того, что Род сказал... что Алан сказал о том, о чем мы сейчас говорим, так сказать, когда речь идет о фишинге или распространении вредоносного ПО. Так сказать, что если сайт был взломан и теперь через него распространяют порнографию? И я даже не хочу говорить... давайте я перефразирую — детскую порнографию, чтобы мы еще об этом не спорили. Так сказать, те очевидные примеры, в отношении которых мы как сообщество все решили, то есть не пограничные примеры. Так что давайте для примера возьмем материалы, связанные с сексуальной эксплуатацией детей, потому что я видела это в моей практике, когда веб-сайт был взломан и стал отображать детскую порнографию. И как... я буду больше говорить о небольших компаниях, чем о крупных, потому что в крупных компаниях, опять же, другие схемы принятия решений, когда речь идет о реагировании на что-то. А небольшие

компании... небольшие компании могут быть заинтересованы в том, чтобы сказать: «Мы не хотим, чтобы это доменное имя ассоциировалось с детской порнографией. Мы это доменное имя рекламируем. У нас на этом доменном имени SCO». Это нужно немедленно прекратить. Мы должны это остановить. Мы должны это отменить. Это то, что я хочу сказать — не существует какого-то одного универсального решения для всех взломанных доменных имен. Я думаю, что лучшее, что мы можем сделать... извините, я слишком быстро говорю. Я сейчас же начну говорить медленнее. Прошу прощения. Это пробились мои корни с восточного побережья США. Прошу прощения.

Я хочу сказать — медленнее сказать, — что при принятии решений в отношении взломанных доменов нужно учитывать множество нюансов. Мы не можем делать предположения о том, чего хочет или не хочет владелец бизнеса, это к тому, что вы сказали, Алан, за исключением каких-то крайних случаев.

Но их нельзя отбрасывать, и точно нельзя отбрасывать... и мне очень нравится то, что делает Tucows, когда

обменивается с реселлерами максимумом информации и объясняет им, что происходит.

Я думаю, что значительная часть проблемы с определением баланса ущерба — это то, что нам нужно учитывать соображения времени, в зависимости от того, сколько вреда наносится и где, а также нужно учитывать интересы владельца, который вполне может решить, что в его интересах этот домен приостановить, чтобы сбросить все, что было, чтобы его маркетинговая поддержка, рекламная поддержка это домена не разбавлялась, это термин из области товарных знаков. Но в этом смысле, я хочу сказать, что во всех прочих аспектах нормальный, респектабельный бизнес может быть разрушен из-за таких случае взлома или заражения, которые мы наблюдаем в нашей практике.

Надеюсь, это было достаточно медленно.

ГРЭМ БАНТОН: Спасибо, Лори.

На очереди Крис, а затем Алан. А потом у меня будет вопрос, который я хотел бы задать участникам дискуссии.

Крис.

КРИС ЛЬЮИС-ЭВАНС: Да, спасибо. Я считаю, что для меня, по нашему вредоносному домену, группа заинтересованных сторон-регистраторов группы заинтересованных сторон регистратур и регистраторов проделали замечательную работу, когда внесли нашу рекомендацию в те стандарты доказательств, которые они применяют к сообщениям о злоупотреблениях.

А для взломанных доменов такая работа на самом деле не проводилась. И я считаю, что в данном случае, чтобы регистратуры и регистраторы могли действовать, должны быть какие-то стандарты доказательств, которые нужно дополнительно объяснить в случаях взломанных доменов.

То есть, так сказать, если мы сообщаем о злоупотреблениях, можем ли мы сказать, что мы связались с поставщиком услуг хостинга, мы связались с регистратором, но ничего не было предпринято? Продолжительность этого можно обсуждать, и, опять же, все сводится к тому, какой ущерб наносится.

Если, так сказать, сосредоточиться на той узкой области, которой мы занимаемся, то это вредоносное ПО, знаете, на данный момент распространяется много программ-вымогателей. Одно-единственное заражение программой-вымогателем может положить конец чьему-то бизнесу, многие сотрудники потеряют работу.

То есть нужно иметь возможность сформулировать должные стандарты доказательств, мы недавно провели большую операцию против Amotech, чтобы остановить тот огромный ущерб, который наносился компаниям и частным лицам. Важно, чтобы это можно было сформулировать, что мы связались с владельцем домена, мы связались с поставщиком услуг хостинга, но ничего не произошло, поэтому теперь мы обращаемся к вам, то есть к регистратору или регистратуре, с просьбой приостановить ввиду этого этот домен — таким образом этот процесс принятия решений может работать.

И мы также понимаем, что затем это может перерасти в дискуссию, понимаете? Это крупная транснациональная компания, и вы просите нас приостановить работу ее

домена. Это будет иметь огромные последствия. На самом деле эта фишинговая кампания нацелена всего лишь на пару человек. Это очень маленький, нишевый рынок, а последствия будут огромными. Пожалуйста, давайте дадим владельцу домена еще 48 часов на ответ, а мы будем просить еще настойчивее.

То есть, на мой взгляд, в случае с взломанным доменом здесь будет большой элемент дискуссии. Это действительно позволяет уменьшить вред, причиняемый взломанным доменом как в результате основной проблемы, так и в виде сопутствующего ущерба.

И да, в таком случае от тех, кто сообщает о злоупотреблениях, потребуют предъявить больше доказательств, но это также потребует и несколько большего участия от тех, кто находится в цепочке принятия решения о мерах по борьбе с этим.

ГРЭМ БАНТОН: Спасибо, Крис. Очень насыщенный ответ.

В данном... я думаю, вы совершенно правы, в этом направлении нужно еще очень много чего сделать. Кроме того, это очень часть распространяется за пределы ответственности или сферы компетенции регистратур и регистраторов и затрагивает таких действующих лиц, как поставщики услуг хостинга. И это вопрос, к которому я хотел бы еще вернуться.

Но сначала Алан, прошу вас.

АЛАН ВУДС: На самом деле после того, что сказал Крис, мне осталось сказать меньше, потому что я могу просто сказать одно... я удивил и себя, и Криса. Мы оба занимаемся этим, работаем над документом SAC115. И мы обсуждаем вопросы функциональной совместимости, чтобы можно было гарантировать, что конкретный оператор подключится к этому в нужный момент, потому что наша цель в данной ситуации — срок жизни конкретного домена. Чем меньше этот срок, тем меньше вреда будет нанесено.

И если обратиться не к тому провайдеру не в тот момент, то этот срок будет больше. А нам нужно пытаться этого

избежать. Так что тут привет, конечно же, Институту злоупотреблений DNS и его будущим усилиям. С нетерпением этого ожидаю. С нетерпением ожидаю возможности связать мою платформу технологической поддержки с вашей, чтобы можно было все это делать.

Но я только хочу указать на один момент, который я тоже пропустил, а именно, что некоторые владельцы доменов являются пользователями крупных платформ, которые сами тоже поддерживают весьма сложные процедуры борьбы со злоупотреблениями.

Я знаю, что вы, Крис, отчасти это тоже упомянули.

Что мы можем приостановить — я приведу очевидный пример, если уж показывать пальцем — facebook.com. Я это скажу. Я не домен .COM. Мы же не отключаем домен facebook.com из-за злоупотреблений, которые имеют место в Facebook. Это было бы смешно. Так что я считаю, что нам нужно очень осторожно применять такой подход.

ГРЭМ БАНТОН: Спасибо, Алан.

Итак, здесь несколько раз поднимался вопрос, который я задам опять Алану и Редж, потому что, мне кажется, это нужно немного разъяснить сообществу: В каких отношениях вы как регистратура или регистратор состоите с поставщиками услуг хостинга? Потому что мне кажется, что многие считают, что это очень тесные отношения. И я не хочу говорить за вас, но мне кажется, что бывают разные обстоятельства, в которых это не так.

Так что, знаете, если мы говорим о сложности этого… а Крис говорит о каналах передачи разрешения проблем между владельцем домена, поставщиком услуг хостинга, регистратором, регистратурой — всегда ли очевидны эти взаимоотношения? Есть ли какие-то стандарты для этой процедуры? Есть ли что-то, в отношении чего нам нужно поработать больше? Редж.

РЕДЖ ЛЕВИ: Спасибо, Грэм.

Опять же, мой ответ будет обусловлен тем фактом, что компания Tucows в первую очередь является оптовым регистратором.

То есть для других регистраторов ответ может отличаться. У нас нет услуг хостинга, поэтому у нас есть Exact Hosting. Это наш филиал, у которого есть приблизительно 500 веб-сайтов. Так что, по сути, я могу сказать, что хостинга у нас нет.

[Смех]

Наши реселлеры, как правило, также предоставляют услуги хостинга. То есть часто получается так, что мы можем обратиться к определенному реселлеру и сказать, мол, вот этот сайт взломан, и они займутся этой проблемой, даже не привлекая к этому владельца домена. То есть в том случае, если наш реселлер является поставщиком услуг хостинга, то такие отношения между нами есть и это тесные отношения.

Однако это не всегда так. И компаний-поставщиков услуг хостинга есть много. Я хочу сказать, что хостинг — это такая служба, которой нужно доменное имя. Но это совершенно

отдельная служба, не связанная с предоставлением услуг регистрации доменных имен.

Так что в том случае, когда наш реселлер не является поставщиком услуг хостинга, все становится сложнее. И нам нужно использовать инструмент DiG, как если бы мы были просто обычным пользователем Интернета, чтобы выяснить, у какой хостинговой компании расположен этот домен, а затем, используя только ту информацию, которую мы сможем найти с помощью инструмента DiG, мы должны связаться с этой компанией.

ГРЭМ БАНТОН: Извините, у меня пропал курсор мыши.

Спасибо, Редж. Я передам слово Алану... а потом подведу итог. Алан.

АЛАН ВУДС: Спасибо. Еще раз извинения нашим переводчикам. Я знаю, что ирландцы говорят быстро.

С точки зрения регистратуры все гораздо сложнее. У нас на самом деле нет никакой связи с поставщиком услуг хостинга. Мы бы, наверное, рассчитывали, что с ним уже свяжутся, прежде чем очередь дойдет до нас. Кроме того, мы бы, наверное, попросили бы наших друзей-регистраторов попробовать связаться с ними, если они также предоставляют услуги хостинга.

Я, однако, скажу, что... у меня тут собака сильно храпит.

Я, однако, скажу, что мы действительно с ними взаимодействуем, насколько это возможно в рамках внешнего взаимодействия. То есть, разумеется, разговор ведется по нескольким темам. Одна из таких дискуссий лежит в контексте ICANN, но есть, например, также такие организации, как Internet & Jurisdiction Policy Network, членами которой мы также являемся, потому что в этой дискуссии участвуют также поставщики услуг хостинга, потому что обычно они не участвуют в контексте работы ICANN. Мы можем вести такой диалог, который позволяет наводить мосты между нами и поставщиками услуг хостинга по таким темам, как Интернет и юрисдикция.

Однако я считаю, что для нас важно затем с этим опытом возвращаться в сообщество ICANN и информировать его о том, чем мы занимаемся. И это, на мой взгляд мы делаем все чаще. Так было в том, что касается определения темы «Интернет и юрисдикция», которое было передано сторонам, связанным договорными обязательствами, и мы над этим работали.

То есть мы работаем с поставщиками услуг хостинга, насколько это возможно, а затем возвращаемся с этим в сообщество ICANN, и это важный результат в том числе для нас как для регистратур.

ГРЭМ БАНТОН: Спасибо, Алан. Мне кажется, что многие регистраторы предоставляют услуги хостинга, но не все. Но это не обязательно что-то очень распространенное, предоставление услуг хостинга или отношения с ними, если учитывать, как много их есть в мире. То есть это реальная проблема, о которой нам нужно начать размышлять, то есть как нам усовершенствовать этот процесс сообщения о злоупотреблениях поставщикам услуг хостинга. Нам нужно,

чтобы в их распоряжении было гораздо больше инструментов и чтобы они были более подготовлены к принятию мер. И еще, как нам определить каналы передачи разрешения проблем для регистратур и регистраторов в тех случаях, когда не отвечает владелец домена или поставщик услуг хостинга? И нам нужно провести повторную оценку поступившего сообщения о нарушении.

Я вижу, что Лори подняла руку, а у нас остается 18 минут. Так что, я думаю, после этого мы попробуем перейти к тому, чтобы непосредственно ответить на некоторые из заданных вопросов.
Лори, прошу вас, вам слово.

ЛОРИ ШУЛЬМАН: Спасибо. Я хотела сказать кое-что, опять же, продолжая дискуссию в чате, насколько у меня это получится.

Но я считаю, что когда речь идет о сообщениях о нарушениях, о функциональной совместимости, о создании безопасных пространств, я действительно считаю, что в эту дискуссию нужно добавить также вопрос о том, какие инвестиции в это пространство можно считать разумными и можно или

следует ожидать в том, что касается технологий борьбы со злоупотреблениями. Или это могут быть люди.

Как сказала Редж, искусственный интеллект работает слишком широко. Регистратор EURid очень открыто заявлял это о работе с искусственным интеллектом. Для проверки результатов работы искусственного интеллекта по-прежнему требуется целая армия людей. Никто не принимает эти результаты за нечто само собой разумеющееся. Они ожидаемы. Мы понимаем, что для более безопасного Интернета... по крайней мере моя группа интересов понимает, что для более безопасного Интернета может потребоваться гораздо больше инвестиций, что может привести к повышению цен. Хотим ли мы это обсудить? Я знаю, что это вызывает обеспокоенность у многих, в особенности у гражданского общества, для которого важно, чтобы цена на доменные имена оставалась относительно низкой и доступной для всех, кому может понадобиться домен и кто может захотеть завести ничего не нарушающий сайт.

Однако в тоже время нам известно, что есть определенные регистратуры... и регистраторы, которые вкладывают

больше средств. Окупаются ли такие вложения? Я считаю, что это важный вопрос, который сообщество должно ставить перед собой.

ГРЭМ БАНТОН: Спасибо, Лори. На самом деле это, пожалуй, хорошее вступление к следующему набору вопросов, которые касаются того, что обсуждается сейчас с помощью функции вебинара Q&A, а также в чате, а именно: Какова роль в этом сообщества? Должна ли ICANN сыграть какую-то роль в попытках решить некоторые из тех проблем, которые мы сегодня здесь подняли. Это могли бы быть какие-то практические рекомендации по борьбе со злонамеренной регистрацией. Как далеко простираются полномочия ICANN, когда речь идет о взломанных доменах? Что мы можем сделать с этим? Какие части сообщества? Я... у меня есть множество вопросов, которые я хотел бы обсудить в контексте DNSAI, но я хотел бы вернуться к этому через минуту.

Мне интересно, есть ли какие-то идеи у наших участников обсуждения в отношении того направления, в котором, по вашему мнению, должно двигаться наше сообщество. А еще

я давно не слышал Рода. Мне любопытно, есть ли у вас какие-то идеи на этот счет. Редж, вы подняли руку.

Прошу вас, говорите.

РЕДЖ ЛЕВИ: Спасибо. Я убеждена, что отдел соблюдения договорных обязательств ICANN в рамках договоров наделен полномочиями обеспечивать исполнение этих самых договоров в тех случаях, когда в отношении злоупотреблений DNS не принимаются меры. То есть меры против того контента, который относится к сфере полномочий ICANN, к которой не относятся, к примеру, материалы, нарушающие закон или связанные с сексуальной эксплуатацией детей, как уже был сказано, но то, что касается злоупотребления DNS. И что ICANN следует больше пользоваться своими полномочиями и этими положениями и на самом деле обеспечивать их исполнение.

ГРЭМ БАНТОН: Спасибо, Редж. На очереди Род, а затем Крис.

РОД РАСМУССЕН: Я уже ответил на этот вопрос. В модуле вебинара Q&A был похожий вопрос, и я на него ответил. Кажется, его задал Фаб.

То есть SSAC действительно упоминал это в документе SAC115, в том месте, где речь шла о том, что свою роль в этом должны играть и корпорация ICANN, и широкое сообщество ICANN, в том числе стороны, связанные договорными обязательствами, все, кто участвует в обсуждении этих вопросов. Но это более широкая тема, а в фокусе нашего внимания, так сказать, конкретно «злоупотребление DNS». Это подмножество всех возможных злоупотреблений в Интернете. И некоторые из сложностей, о которых мы сегодня говорили, о том, какие поставщики услуг должны участвовать в борьбе со злоупотреблениями в зависимости от наносимого ущерба, взломан ли домен или же зарегистрировал специально для нанесения вреда, это очень хорошая дискуссия в этом пространстве, а также... подумать о стандартах доказательств, как долго... или какие существуют ожидания в том, что касается подтверждения и устранения злоупотреблений, о которых сообщается, и какие меры могут приниматься. Есть еще целый ряд тем в этом более широком наборе вопросов.

Мы видим движение в этом направлении. Знаете, у нас есть замечательные инициативы, такие как... Институт злоупотреблений DNS, а также что-то из той работы, которая ведется в организации Internet & Jurisdiction Policy Network. Очень много предпринимается усилия для создания каких-то стандартов, практических методик и т. п., но это еще не готово, и нам еще очень много придется сделать для того, чтобы создать... некую экосистему, в которой можно было бы ожидать чего-то в отношении процедуры, соотношения и прочих факторов, при этом также нужно создать какую-то более совершенную систему для реагирования и предотвращения злоупотреблений любого рода.

Так что, на мой взгляд, важно чтобы мы, сообщество ICANN, в основном сходились в нашем видении этого, а еще нужно организовать взаимодействие с более широким интернет-сообществом для решения этих проблем, потому что если каждый из нас попытается решить ту уникальную часть общей проблемы, которая относится именно к нему, то в результате у нас получится множество различных систем. Но ведется большая и целенаправленная работа, а ICANN может сыграть свою роль в том поддержании этого диалога, потому

что у нее есть ресурсы и охват, в то время как у многих других инициатив, направленных на службы хостинга или электронной почты и т. п., этого всего может не быть.

Так что я настоятельно призываю всех ознакомиться с документом SAC115 и принять участие в тех дискуссиях, которые сейчас ведутся, чтобы проактивно... чтобы подумать глобально над тем, какой подход следует применять для решения этих проблем, и создать те рамочные концепции, которые нам понадобятся для того, чтобы, опять же, задать ожидания и двигаться дальше в соответствии с ними.

Спасибо.

ГРЭМ БАНТОН: Спасибо, Род.

Кажется, я видел, что кто-то уже опубликовал в чате ссылку на документ SAC115, но я на всякий случай попрошу, чтобы это сделали еще раз.

Крис, а затем Алан.

КРИС ЛЬЮИС-ЭВАНС: Да, спасибо. Это снова Крис Льюис-Эванс, для протокола.

Я согласен со всем, что Род здесь сказал, но сначала я хотел сказать, что я согласен с Редж в том, что касается обеспечения соблюдения договорных обязательств. Однако я считаю, что мы, так сказать (неразборчиво) в значительной степени в том, как следует работать со злоупотреблениями DNS, и этот разговор является частью этого процесса. Я не думаю, что у нас есть надлежащая процедура для работы с взломанными доменами, и это одна из важных причин этой дискуссии. Так что было бы, на мой взгляд, очень полезно, чтобы у нас были какие-то минимальные ожидания, а также чтобы это документировалось, чтобы у клиентов была возможность измерять реагирование. И тогда можно было бы предъявлять эти стандарты всем регистраторам и регистратурам, чтобы они понимали, что от них требуется, и это, на мой взгляд, ключевое условие. А также какие-то учебные материалы для них. Знаете, как уже было сказано, есть множество разных видов регистраторов и регистратур, и самое, на мой взгляд, главное — это понимать, как лучше всего на практике с этим работать.

То есть ICANN много чего может сделать для того, чтобы распространить эти усилия по всему, так сказать, ландшафту ICANN. А затем просто отталкиваться от того, что сказал Род... и заниматься информированием в других областях. Так сказать, хостинговые компании, поставщики услуг, мы много раз их упоминали в этом разговоре, а они действительно очень большой, ключевой компонент реагирования на ту часть этой проблемы, которая касается DNS.

Спасибо.

ГРЭМ БАНТОН: Спасибо, Крис.

Алан, кратко, а затем мы попытаемся ответить на несколько вопросов, заданных через функцию вебинара Q&A, прежде чем подведем краткий итог.

АЛАН ВУДС: Отлично. На самом деле очень кратко. Так получается, что, так сказать, в рамках всего этого процесса, и даже еще до

того, как мы предложили провести это пленарное заседание, подгруппа о злоупотреблениям DNS группы заинтересованных сторон-регистратур на самом деле приступила к работе над созданием какого-то документа, по меньшей мере, чтобы начать этот процесс. Грэм, конечно же, в этом участвует. В данный момент он неформальный лидер в этой работе и, кажется, мы приглашаем к этому людей в том числе и из SSAC. То есть мы хотим привлечь Рода и, кажется, Джеффа Бедсера (Jeff Bedser), чтобы мы могли провести какое-то серьезное обсуждение различий между злонамеренными регистрациями и взломанными доменами, чтобы сделать именно то, о чем только что говорил Крис, — попытаться заложить основу.

Это всегда была открытая дискуссия. Этим мы признавали, что это однозначно проблема, так сказать, злоупотребления DNS, и мы работаем над этим, но нам нужно также поработать над этими нюансами и различиями, которые там есть, чтобы мы могли решить эту проблему эффективно.

Так что я бы сказал — следите за этим, я надеюсь, вскоре мы что-то подготовим по этому вопросу, чтобы положить этому какое-то прочное и надежное начало.

ГРЭМ БАНТОН: Спасибо, Алан. То есть этот документ, над которым мы работаем, — это TPH по этой теме. Я думаю, мы на самом деле постараемся выпустить его до конференции ICANN74, которая пройдет в Гааге в июне. Я думаю, это получится скорее ближе к июню, но мы точно распространим его в сообществе.

Фаб уже давно задал вопрос в чате примерно по этой теме. Так сказать, что может сделать сообщество? Можно ли внести в соглашение об аккредитации регистраторов какие-то изменения, чтобы зафиксировать что-то из таких практических методик или мер по борьбе с теми проблемами, о которых мы сегодня говорим? Потенциально. Я думаю, конечно же, такой вариант можно обсуждать.

Вчера я получил письмо от Института проблем злоупотреблений DNS, это такое обращение от малой группы DNSO по проблемам злоупотреблений DNS, в котором задается практически этот же вопрос. Я сам постоянно это обдумываю, и я считаю, что сообщество могло бы сыграть здесь свою роль в том, чтобы на самом деле повыбирать

какие-то маленькие удобоваримые фрагменты из этих более масштабных проблем. Мы много говорили о сложности этой экосистемы, особенно в тех случаях, когда злоупотребления осуществляются через взломанные домены. И я считаю, что нам нужно начать, пожалуй, с самого доступного со стороны злонамеренных регистраций, тогда, если что-то пойдет не так, то и последствия будут не такие серьезные, и жертв будет меньше.

То есть я считаю, что мы можем начать думать о том, что из этой работы над проблемой злонамеренной регистрации взять себе в сообщество. И я думаю, что так это еще и больше будет соответствовать Уставу ICANN. То есть я бы предложил это, и я надеюсь, что это также отвечает на вопрос Фаба в чате.

Давайте посмотрим... у нас остается семь минут. Я хочу дать всем возможность подумать, возможно, кто-то хочет что-то сказать в завершение, или, возможно, в модуле функции вебинара Q&A есть какой-то вопрос, на который кто-то хотел бы ответить непосредственно.

Редж подняла руку. Вам слово, Редж.

РЕДЖ ЛЕВИ: Спасибо, Грэм. Я хотела подчеркнуть то, что Эшли на самом деле сказал в чате, что группа заинтересованных сторон-регистраторов в настоящее время работает над инструментом, в который можно было бы ввести доменное имя, а он выдал бы всю информацию о том, кто предоставляет соответствующему сайту услуги хостинга и как с таким поставщиком связаться.

Так что следите за этим. Чуть раньше на этой неделе мы уже провели премьерный показ для нашей группы заинтересованных сторон-регистраторов, но мы надеемся, что в ближайшее время сможем дать ссылки для всех.

ГРЭМ БАНТОН: Спасибо, Редж.

Я думаю, это важно, и это похоже на то, над чем сейчас работает также Институт проблем злоупотребления DNS, это будет некий централизованный инструмент для сообщения о злоупотреблениях. Совершенно очевидно, что все эти процессы, связанные с тем, чтобы определить всех

участников этой экосистемы — кто они, как с ними связаться, какие стандарты используются для связи с ними — все это на данный момент довольно запутанно. И мы все вместе можем сделать это лучше, просто взять это в свои руки, так сказать, эти процессы и эту проблему контактных данных, и сделать все это немного проще. И я работаю над чем-то подобным. Сейчас я об этом говорить не буду, но позже я поделюсь новостями об этом.

Итак, давайте посмотрим, возможно, мы сможем очень кратко ответить на один или два вопроса. Еще раз прошу прощения за то, что мы так и не добрались до тех дополнительных вопросов, которые у нас были.

Возможно, пока я буду зачитывать эти вопросы из очереди, я также попрошу участников дискуссии сказать, возможно, у кого-то есть какие-то заключительные мысли по этому вопросу... по этой теме, которую мы сегодня здесь обсуждаем.

Я вижу руку Лори. Прошу вас, говорите.

ЛОРИ ШУЛЬМАН: Разумеется. Спасибо.

В чате все происходит так быстро, что я уже за этим не успеваю. Но я хочу сказать, что это очень своевременная и очень необходимая дискуссия. И я хочу поблагодарить организаторов за то, что вы пригласили группу интересов по вопросам интеллектуальной собственности и лично меня, потому что здесь действительно были подняты сложные проблемы.

Я не думаю, что кто-то скажет, что они простые. Это непростая тема. Я не думаю, что кто-то предложит нам спешить с принятием решений. Но я действительно считаю, что, по крайней мере, с моей позиции, нам не следует... в особенности в случае с взломанными доменами. Сейчас сообщество столкнулось с тем, что специалисты по охране товарных знаков, правоохранительные органы и специалисты в области безопасности знали все эти годы, — что в каждом случае злоупотреблений может быть своя фактология. Для каждого случая злоупотреблений могут быть какие-то меры, которые лучше или хуже. Каждый случай злоупотреблений будет рассматриваться в контексте своего специфического набора фактов.

При всем этом для меня очевидно, что на нас как сообщество возложена ответственность за формирование нормы. И именно в этом, на мой взгляд, такие проекты, как Internet & Jurisdiction Policy Network, такие документы, как SSAC115, а также та работа, которую выполняете вы, Грэм, — все это действительно помогает задать эту норму.

Но следующий компонент этой картины, и я думаю, что можно это так сказать, те нормы, которые устанавливаются за пределами нашего сообщества, как они работают в пределах ICANN? И какого рода... я написала в чате такое очень далеко идущее предложение, которое обсуждалось в моей группе интересов, это то, что... когда мы столкнулись с проблемой кибер... извините, кибersквотинга, это было 20 лет назад и тогда не было правовой системы или инстанции, принимающей решение, которые могли бы помочь в таких случаях. И мы нашли много параллелей с единой политикой разрешения споров о доменных именах, или UDRP, которая замечательно работала 20 лет.

Не пришло ли время подумать о какой-то процедуре, аналогичной UDRP, но для взломанных доменов? И на этом я

остановлюсь, но я считаю, что это вопрос на будущее, когда мы будем говорить о решениях и нормах, это стоит обсудить.

ГРЭМ БАНТОН: Спасибо, Лори. Спасибо за ваш комментарий. Замечательное слово вы употребили, futuring, когда говорили о будущем.

Прежде чем я передам слово Алану, я хочу кратко ответить на вопрос от Гриффина в чате, отчасти мы его, на мой взгляд, уже затрагивали, он звучит так: работа... в пределах сообщества, для меня как для человека, возглавляющего институт, занимающийся этой проблемой, и я знаю, что есть еще несколько человек, и для меня это... совершенно очевидно, что проблемы злоупотреблений очень быстро выйдут за пределы сферы полномочий ICANN, в тех ситуациях, когда нам нужно будет взаимодействовать с поставщиками услуг хостинга. У нас есть несколько организаций, таких как Global Cyber Alliance, Internet & Jurisdiction Policy Network, Институт проблем злоупотреблений DNS, инициатива topDNS интернет-ассоциации eco, которые работают аналогичным образом и над аналогичными проблемами. И мы должны разобраться в

том, как работать вместе. Я думаю, что мы все вместе поддерживаем модель работы с участием многих заинтересованных сторон и ICANN, и четко понимаем, так сказать, очевидную важность такой работы.

Но мы должны также понимать, что здесь есть место также для смежных организаций, которые могут выходить за эти пределы и взаимодействовать с более широким сообществом таким образом, который, возможно, не подошел бы для ICANN или для правил, действующих в системе ICANN.

То есть они могут объяснять внешним интересам, это могут быть, так сказать, регуляторы по всему миру, а также ICANN в рамках сообщества, что есть место как для работы в пределах сообщества, результатом которой являются договорные обязательства, процессы разработки политик и т. п., и для отрасли, чтобы вырабатывать оптимальные практические методики, устанавливать контакты со смежными организациями, то есть с поставщиками услуг хостинга и электронной почты, с такого рода сообществом, чтобы все они могли сотрудничать и работать сообща. И нам просто

нужно делать это лучше, потому что это пойдет на пользу всем и позволит решить множество таких проблем.

У нас осталась одна минута. Похоже, что вы, Алан, будете выступать последним.

АЛАН ВУДС: Я только хочу повторить то, что говорили здесь вы, Грэм. И я считаю, что важно просто... я не возражаю против того, что сказала с Лори. На самом деле я очень даже согласен с тем, что она сказала. Я думаю, нам просто нужно сделать так, чтобы UDRP была для доменных имен... позволяла решать проблему доменных имен. То, что мы пытаемся здесь решить, это буквально то же самое, о чем говорит Грэм, что это выходит далеко за рамки просто регистратур и регистраторов. Мы говорим о поставщиках услуг хостинга, об этой стороне системы ICANN. То есть это шире, чем собственно ICANN, но это определенно соотносится с группами интересов в ICANN, и мы можем делать свое дело и сотрудничать с другими, чтобы попытаться прийти к решению этой проблемы. И я думаю, что мы буквально так и пытаемся сейчас действовать, из того, что мы понимаем в этой области функциональной совместимости. Нам нужна поддержка и понимание со всех сторон. И мы делаем это все

лучше и лучше. Я действительно считаю, что мы делаем это лучше. И мы должны продолжать стремиться совершенствоваться.

ГРЭМ БАНТОН: Спасибо, Алан.

У нас закончился час. Большое спасибо всем участникам дискуссии. Спасибо, что нашли для нас время. Мацей, спасибо за вашу прекрасную презентацию. Аудитория, вы были великолепны, вы придерживались выбранной нами сегодня темы и предложили нам гораздо больше вопросов и комментариев, чем мы были в силах разобрать. Приношу свои извинения. Мы попытаемся какие-то из них записать и посмотрим, возможно, их можно будет как-то включить в какое-то другое заседание или еще какую-то работу.

Я думаю, что на этом мы можем закончить наше сегодняшнее заседание. Большое всем спасибо за такое активное участие. Я очень это ценю.

[КОНЕЦ СТЕНОГРАММЫ]