АБУ-ДАБИ — сквозное заседание сообщества: Информирование о злоупотреблении DNS для разработки политик и противодействия
Понедельник, 30 октября 2017 года, 13:30 – 15:00 по GST
ICANN 60 | Абу-Даби, Объединенные Арабские Эмираты

ИРАНГА КАХАНГАМА (IRANGA KAHANGAMA): Добрый день! Пожалуйста, займите свои места, мы собираемся начинать через несколько секунд.

Спасибо.

Хорошо. Я хочу поблагодарить всех, кто пришел сегодня, на сегодняшнее заседание, посвященное информированию о злоупотреблениях для выработки политик на основе фактов и эффективного противодействия злоупотреблению DNS. Меня зовут Иранга Кахангама, я один из организаторов данного мероприятия от имени Федерального бюро расследований США вместе с рабочей группой по общественной безопасности, я также член рабочей группы по общественной безопасности.

Вместе со мной сопредседатель также Кэтрин, хотите представить свои организации?

КЭТРИН БАУЭР-БУЛЬСТ (CATHRIN BAUER-BULST): Разумеется. Меня зовут Кэтрин Бауэр-Бульст. Я являюсь одним из сопредседателей рабочей группы GAC по вопросам общественной безопасности, я представляю Европейскую комиссию.

ИРАНГА КАХАНГАМА: Спасибо, Кэтрин.

Итак, я сейчас сделаю следующее: я очень кратко расскажу о предыстории и логике этого мероприятия и о том, что мы надеемся из этого получить, а затем Кэтрин перейдет к вопросам, связанным больше с логистикой и деталями организации этого мероприятия.

Это взгляд, с точки зрения рабочей группы по общественной безопасности, на естественную эволюцию того, как смещался фокус внимания в вопросах злоупотреблений DNS и противодействия таким злоупотреблениям, которые мы попытались в общих чертах представить сообществу ICANN. Это естественное развитие других вопросов, которыми мы занимались, в том числе тех различных вопросов, которые задавались в формате рекомендаций GAC по проблемам злоупотреблений DNS, а также ряда других дискуссий и мероприятий, которые мы проводили.

Когда вышло объявление о проведении сквозных заседаний сообщества, мы, разумеется, были очень заинтересованы в этом, и я считаю, что стало совершенно очевидно наличие в

сообществе большой заинтересованности в том, чтобы подробнее обсудить эту проблему и двигаться дальше на пути поиска решения некоторых из этих проблем.

Итак, чтобы дать вам... краткая предыстория: у нас было три телеконференции в рабочей группе, от добровольных участников до различных сообществ заинтересованных сторон, которые вы можете видеть здесь в этой таблице, и мы... мы поставили себе задачу на этой конференции определить, как двигаться дальше.

Сначала рабочая группа по общественной безопасности выработала концепцию принципов, на основе которых следовало бы попытаться каким-то образом консолидировать работу над вопросами злоупотреблений DNS.

После того, как некоторые из них были предложены, стало очевидно, что, по всей видимости, существует множество различных точек зрения на эти вопросы, так что логичным результатом этого мероприятия стало понимание того, что нам следует обсудить эти вопросы с более широким срезом представителей сообщества, чем то, что можно наблюдать здесь сегодня.

Поэтому мы сделали следующее — мы организовали это заседание и составили список проблем, касающихся борьбы со злоупотреблениями DNS, которые мы разделили на три категории: обнаружение злоупотреблений DNS,

информирование о злоупотреблениях DNS, а также статистические данные и то, как их использовать.

То есть мы собираемся запланировать и пригласить аудиторию к участию в заседании, которое будет посвящено этим трем общим темам, и мы надеемся, что по итогам этого заседания у нас получится перейти к какому-то подходу на основе принципов, в рамках которого продолжится участие в этой работе рабочей группы по общественной безопасности и остального сообщества.

Спасибо.

КЭТРИН БАУЭР-БУЛЬСТ: Мы переходим к следующему слайду, и позвольте мне вкратце представить вам эту тему. Однако сначала мы заслушаем два коротких выступления Дэвида Конрада (David Conrad) и Дрю Бэгли (Drew Bagley), которые сидят слева от меня, если смотреть из аудитории, а затем у нас состоится обсуждение в комиссии, составленной из представителей различных групп, участников от различных групп, которые также внесли свой вклад в работу, предшествующую этому заседанию, в подготовку того, о чем говорил Иранга. Итак, у нас есть Алан Вудс (Alan Woods) из группы заинтересованных сторон-регистратур, у нас есть Грэм Бантон (Graeme Bunton) из группы заинтересованных сторон-регистраторов, у нас есть Таня Тропина (Tania Tropina) из группы интересов

некоммерческих пользователей (NCUC), Дэниз Мишель (Denise Michel) из группы интересов коммерческих пользователей, Джонатан Матковски (Jonathan Matkowsky) из группы интересов по вопросам интеллектуальной собственности (IPC), Род Расмуссен (Rod Rasmussen), вступающий в должность председателя SSAC, и Джейми Хедлунд (Jamie Hedlund), который занимает должность вице-президента ICANN по вопросам соблюдения требований и механизмам защиты прав потребителей.

Следующий слайд, пожалуйста.

Итак, как сказал Иранга, мы пытаемся структурировать эту дискуссию, поэтому это заседание будет организовано следующим образом: мы начнем с двух коротких докладов, а затем мы попытаемся пройтись в этой дискуссии по трем категориям, которые уже были названы Ирангой. А в ходе телеконференций, при обсуждении принципов, было высказано следующее: несмотря на то, что пока мы еще не можем прийти к согласию в том, какие принципы должны применяться к информированию о злоупотреблениях DNS, к тому, как будут собираться данные и как мы будем их впоследствии использовать, было очевидно, что такие принципы, которые будут применяться к этому процессу, должны соответствовать трем ключевым вопросам, вы можете видеть сейчас эти вопросы на этом слайде, мы вернемся к этому в нашей дискуссии после двух докладов, с

которых она начнется. И эти вопросы, это, во-первых, каким образом можно надежно выявлять злоупотребление DNS? Затем, исходя из этого, как нам создать эффективные и прозрачные средства информирования о злоупотреблениях, чтобы сделать доступными эти данные? И потом третье: как нам затем использовать эти данные?

Вот это те три вопроса, которые мы надеемся обсудить с вами сегодня. Так что, несмотря на то, что у нас есть очень большая комиссия признанных специалистов в этой области, мы очень хотим привлечь вас к участию в этом мероприятии.

Итак, сейчас у нас будут эти два коротких доклада, в качестве старта. Затем мы начнем обсуждение по каждому из разделов с вопроса к одному из членов нашей комиссии. И когда мы будем отвечать на этот вопрос, задавать его, мы хотим пригласить вас... если вы хотите добавить свое мнение к общему вопросу, который будет задаваться по этой категории, или к конкретному вопросу, который мы будем обсуждать с членами комиссии, пожалуйста, скажите об этом кому-то из членов персонала ICANN, которые будут присутствовать в аудитории с микрофонами. Вы можете видеть, как они держать эти номера здесь, так что, пожалуйста, просто поднимите руку. Кто-то из них подойдет к вам и даст нам знак, что вы хотите сделать заявление, и мы предоставим вам такую возможность.

Мы хотели бы предоставить возможность высказаться как можно большему количеству участников, поэтому мы ограничим время выступления двумя минутами для каждого. Это также относится и к членам комиссии. Мы постараемся обеспечить равные возможности для всех, насколько это возможно. Пожалуйста... Прошу вас, высказывайтесь и делитесь в нами вашими мнениями.

А теперь без дальнейших разглагольствований мы перейдем к первому из докладов, который посвящен платформе отчетности о случаях злоупотребления доменами, его нам представит Дэвид Конрад.

Дэвид, вам слово.

ДЭВИД КОНРАД: Большое спасибо.

Я Дэвид Конрад, технический директор ICANN. По теме этой дискуссии: мы в моей группе и в офисе технического директора разрабатывали нечто, что иногда называют платформой отчетности о случаях злоупотребления доменами.

Следующий слайд, пожалуйста. О, это я. Ха. Вот так.

Итак, основные моменты. Что такое платформа отчетности о случаях злоупотребления доменами, которую мы предпочитаем называть DAAR, потому что так гораздо короче.

Это такая система, которая позволяет предоставлять данные о регистрациях и злоупотреблениях, связанных с доменными именами, регистратурам и регистраторам доменов верхнего уровня. Сейчас она больше ориентирована на домены gTLD, потому что по ним у нас были данные, которые можно было анализировать, однако система не обязательно должна этим ограничиваться. Если домены ccTLD захотят в этом участвовать, то мы будем рады обсудить это с ними.

Чем система DAAR отличается от других систем отчетности? Я уверен, что многим из вас известно, что механизмов отчетности существует огромной множество, некоторые из них… на самом деле большинство из них связаны с теми или иными коммерческими продуктами или услугами.

Мы делаем следующее: мы изучаем все регистратуры и регистраторов gTLD, от которых мы можем получать данные. Мы… в отличие от большинства основанных на репутации… или от большинства случаев, когда проводится такой анализ, мы пытаемся использовать большое количество источников данных, это каналы репутационных данных, их также называют блок-листами или RBL-списками.

Мы также собираем эти данные за определенный период времени, чтобы поддерживать достаточный объем данных для проведения исторических исследований.

Мы обычно рассматриваем, или, на самом деле, мы обязаны рассматривать множество различных угроз. Основное внимание мы уделяем угрозам, которые были определены в Пекинском коммюнике GAC, это фишинг, управляющие серверы ботнетов, а также распространение вредоносного ПО, кроме того, мы включаем в наш анализ спам, что, правда, вызывает определенные разногласия. Мы включили спам в первую очередь потому, что это очень эффективный транспорт для осуществления остальных видов нарушений, кроме того, это позволяет нам составить некий указатель и получить информацию, потому что обычно, когда тот или иной домен верхнего уровня оказывается под воздействием того или иного вредоносного ПО или иного вида деятельности злоумышленников, он также подвергается воздействию спама.

Мы также — это важный момент — пытаемся использовать научный подход, обеспечивать максимальную прозрачность и воспроизводимость. Зарождение проекта DAAR пришлось приблизительно на тот момент, когда один из поставщиков оборудования для обеспечения безопасности представил отчет, в котором было показано количество доменов gTLD, на 100% связанных со злоупотреблениями или нарушениями, и в некоторых из этих отчетов был такой комичный момент, когда один из них был на 100% связан со спамом, и это была зона, состоявшая из одного домена, домена верхнего уровня .NIC,

однако поскольку получилось так, что этот домен верхнего уровня совпал со строкой, по которой выполнял поиск этот поставщик оборудования для обеспечения безопасности, кажется, .ZIP, это привело к тому, что все домены в этом домене верхнего уровня были классифицированы как вредоносные.

Когда СМИ... когда этот отчет вышел, СМИ на него просто набросились. Он на самом деле вызвал множество вопросов, как к ICANN, так и к сообществу в целом. Впоследствии многие представители сообщества обращались ко мне и к ICANN и просили... они на самом деле говорили: «Кто-то же должен вести какой-то авторитетный список. Кто-то должен выработать хорошо документированную методологию, с которой все бы согласились, чтобы мы не получали эти необъективные отчеты, продиктованные коммерческими интересами». То есть это вызвало к жизни первые идеи, из которых в конечном итоге развился проект DAAR.

Следующий слайд, пожалуйста.

Это опять я. Боже мой! Как бы то ни было.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Держать это?

ДЭВИД КОНРАД: Нет, я потом разберусь. Это технические моменты. Я в этом не разбираюсь.

[Смех]

Итак, я уже сказал, что в системе DAAR используется множество источников данных об угрозах. То есть мы собираем те же данные о нарушениях, которые поступают в распоряжение отрасли и пользователей Интернета. Одним из ключевых требований проекта DAAR было то, что что бы мы ни делали… этот проект могли бы воспроизвести другие. Мы не полагаемся ни на какие конфиденциальные данные. Мы не формируем никакие данные самостоятельно. По сути, мы берем общедоступные данные и определяем корреляции, по сути, мы просто составляем такие большие таблицы, в которых документируются различные формы нарушений и злоупотреблений по разным категориям.

Собираемые нами данные о нарушениях используются в коммерческих системах обеспечения безопасности, которые обеспечивают защиту миллионов пользователей и миллиардов почтовых ящиков ежедневно. Сектор науки и образования и отраслевые пользователи… пользуются этой информацией так же, как это делаем мы, они доверяют этим наборам данных. То есть и в исследовательской среде, и в коммерческом секторе для этих наборов данных проверены и

подтверждены точность, надежность глобального охвата и небольшое количество ложноположительных результатов.

Структура, к которой мы пришли для системы DAAR, заключалась в поддержке расширяемой платформы, мы экспериментируем проведение анализа по разным подмножествам данных, просто чтобы обеспечить лучшее понимание того, что там происходит.

Ключевой момент здесь заключается в следующем: DAAR — это инструмент, которые позволяет сообществу, сообществу ICANN, видеть то, как экосистема доменных имен воспринимается за пределами нашего сообщества.

Видите, я не сказал «следующий слайд», меня и не слушаются. Я очень не люблю, когда это происходит. Вот так.

Поступил вопрос о критериях, по которым мы отбираем наборы данных. На этом слайде показаны критерии, которые мы используем в текущей версии DAAR. Среди прочего мы занимаемся тем, что запрашиваем у комитета SSAC мнение о критериях, в соответствии с которыми должны отбираться каналы данных для использования в DAAR, и прямо сейчас мы также занимаемся подготовкой запроса предложений для сообщества… извините, для независимых экспертов, что они думают о нашей методологии. Как только мы получим эту информацию, мы выработаем некий документ, в котором будет описана предлагаемая нами к использованию

методика, и вынесем его на общественное обсуждение. Затем он вернется в рамках обычной процедуры ICANN и мы изменим каналы данных в соответствии с критериями, которые… в соответствии с теми мнениями и комментариями, которые мы получим.

Однако в настоящий момент те наборы данных, которые мы используем, требования к ним таковы, что данный набор данных должен пользоваться доверием со стороны операционного сообщества специалистов по обеспечению безопасности в том, что касается их точности и очевидности в рамках процесса. В частности, любой используемый нами набор данных должен основываться на абсолютно прозрачной процедуре добавления или удаления того или иного доменного имени в блок-лист. Выбранный блок-лист должен обеспечивать классификацию угроз, отвечающую нашим потребностям. То есть основные категории — это ботнеты, распространение вредоносного ПО и фишинг.

Все эти блок-листы пользуются широкой поддержкой в операционном сообществе специалистов по обеспечению безопасности. Это каналы, который встраиваются в коммерческие системы обеспечения безопасности, которые используются операторами сетей, к примеру, в почтовых серверах и т. п., для защиты пользователей и устройств, они используются поставщиками услуг электронной почты и сообщений для защиты их пользователей.

Просто чтобы было ясно — эти репутационные блок-листы, которые мы используем, они на самом деле используются практически всеми. Они используются в браузерах, в облачных службах и системах выдачи контента, в инструментах для работы с социальными сетями, они очень часто используются в DNS. В… где это было? В Копенгагене в рамках заседания с группой технических экспертов у нас на самом деле была презентация, которую провел Пол Викси (Paul Vixie) из компании Farsight Security. Они разработали программное обеспечение, которое использует т. н. зоны политики реагирования, что позволяет блокировать доменные имена через политики.

Нам известно о ряде интернет-провайдеров и поставщиков услуг электронной почты, которые блокируют целые домены верхнего уровня, потому что считают, что в этих доменах полно вредоносного ПО… это вредоносные домены и злоупотребление DNS.

Кроме того, операторы частных сетей используют блок-листы и коммерческие брандмауэры, а также корпоративные системы электронной почты и обмена сообщениями и независимые поставщики услуг электронной почты.

Это список того, что мы используем в настоящее время — я хочу извиниться за то, что я уже превысил лимит времени — в системе DAAR. Так что, по сути, у нас… что это? Семь как бы

основных репутационных блок-листов, или RBL-списков, при этом один из них на самом деле представляет собой составной список, в который входит множество дополнительных.

Итак, почему система DAAR отмечает домены, задействованные в рассылке спама? Это вопрос, который уже несколько раз поднимался.

В Хайдерабадском коммюнике GAC выразил заинтересованность в работе со спамом и, разумеется, мы всегда прислушиваемся к тому, что нам говорят в нашем сообществе. Если говорить реалистично, спам представляет собой основное средство доставки угроз безопасности, а система DAAR измерят упоминания доменных имен в текстовых частях спам-сообщений, а не собственно домены, задействованные для рассылки спама.

На этом я передаю слово Фабьену, или кому? Иранге или Кэтрин?

Кто-нибудь.

КЭТРИН БАУЭР-БУЛЬСТ: Большое спасибо, Дэвид. Дрю. Вы следующий.

ДРЮ БЭГЛИ: Спасибо, Кэтрин. Меня зовут Дрю Бэгли, я представляю фонд Secure Domain Foundation и компанию CrowdStrike. Если отталкиваться от того, что рассказал Дэйв о значимости этих данных и надежности данных такого рода, я хотел бы обсудить то, как мы можем использовать эти данные, чтобы не просто блокировать домены верхнего уровня на операционном уровне, а использовать их в качестве информационной основы при разработке политик, что могло бы действительно помочь усовершенствовать те усилия, которые предпринимаются для поддержки открытого и свободного Интернета, а также не допустить противоречий с идеей универсального принятия, потому что именно это происходит, если не бороться с нарушениями.

Как сказал Дэйв, в сообществе существует консенсус в том, что касается определенных форм злоупотреблений, в первую очередь в отношении фишинга и вредоносного ПО, которые явно запрещены соглашениями, а также в отношении спама, который является распространенным механизмом доставки для таких нарушений.

Поэтому для сообщества при работе со злоупотреблениями в рамках разработки политик важно понимать следующее: нам нельзя завязнуть в различных трактовках того, что мы можем считать злоупотреблениями, потому что это не даст нам на самом деле заняться собственно злоупотреблениями. Вместо этого очень важно нам как сообществу начать работать над

вопросами политик в том, в отношении чего существует консенсус и есть измеримые показатели. И, как это описал Дэйв, есть много надежных измеримых показателей, касающихся фишинга, вредоносного ПО и спама, а также управляющих серверов ботнетов.

В рамках группы по анализу конкуренции, потребительского доверия и потребительского выбора мы рассматривали проблему, которую вызывает злоупотребление DNS, в контексте средств защиты, реализованных для предотвращения злоупотреблений в новых gTLD. И чтобы измерить это на промежуточном этапе, мы рассмотрели фишинг, вредоносное ПО и спам и заказали проведение исследования для анализа данных, аналогичных тем, что представил Дэйв, которые включаются в различные черные списки, а затем извлечь какие-то выводы из такого анализа на макроуровне, чтобы на основе этого выработать рекомендации в отношении политик.

Я использую это как пример, иллюстрирующий то, как такого рода данные могут использоваться для способствования разработке политик на основе данных в сообществе.

В результате… анализа этих данных, продолжавшегося один год, мы пришли к выводу, что на самом деле злоупотребления не являются чем-то совершенно универсальным для всех доменов верхнего уровня. Аналогичным образом это не

случайное распределение. Вместо этого мы на самом деле смогли определить факторы, которые могли влиять на корреляцию с более высоким уровнем злоупотреблений в той или иной зоне или у тех или иных регистраторов или, наоборот, со сниженным уровнем злоупотреблений по тем или иным операторам регистратур или регистраторам.

Так что, скорее всего, неудивительно, что в тех случаях, когда применялось больше ограничений регистрации, из-за чего было труднее зарегистрировать доменное имя, отмечалось… меньше случаев злоупотреблений.

Аналогичным образом по тем регистраторам или операторам регистратур, у которых отмечалась тенденция большей корреляции с очень высоким уровнем злоупотреблений, также обнаруживалось, что они предлагали очень низкие цены и зачастую различные варианты массовой регистрации доменных имен, к чему я еще вернусь через минуту.

Кроме того, при анализе некоторых из этих доменов верхнего уровня на самом низком уровне мы обнаружили сильную корреляцию между использованием терминов товарных знаков в качестве приманки и фишинговыми кампаниями, что, пожалуй, неудивительно. Однако конкретный пример, приведенный в этом отчете, касался 76 доменных имен, в которых использовались различные варианты написания товарных знаков Apple, таких как iPhone, для, так сказать,

проведения таргетированных фишинговых кампаний, нацеленных на пользователей. И эти 76 доменных имен составляли 76 из, кажется, 83 случаев нарушений для данного домена верхнего уровня в том квартале.

И в целом эти данные показали нам то, что, по сути, существует определенный пробел в политиках. И я считаю, что именно поэтому так важно то, что осуществляется в рамках проекта DAAR и чем занимаются другие участники сообщества, чтобы была возможность собирать и анализировать такие большие наборы данных, особенно полагаясь на данные WHOIS, потому что тогда на самом деле будет видно, где в действительности существующие у нас механизмы, возможно, не учитывают все возможные ситуации, с которыми мы сталкиваемся и которые могут фактически влиять на стабильность и отказоустойчивость DNS.

Так что я хочу выделить двух регистраторов, особенно проблемных с точки зрения существующих у нас наборов инструментов, чтобы эта информация могла быть использована для разработки наших политик и движения вперед.

Первый из них — это регистратор, работа которого с тех пор была приостановлена, однако он имел возможность работать большую часть 2016 года, демонстрируя очень высокий

уровень злоупотреблений. И на самом деле к приостановке его работы привело не такое большое количество нарушений. Просто в один прекрасный день они перестали платить по счетам, так еще какие-то проблемы упоминались. Однако, по сути, если вы помогаете киберпреступникам, просто платите по счетам, возможно, вам еще долго ничего не будет. На мой взгляд, это один из уроков в этой ситуации.

Еще один момент, который подчеркнула эта ситуация, — это то, что когда используется модель на основе жалоб, когда мы ожидаем реагирования, потому что такой подход используется в отношении злоупотреблений DNS, то на самом деле может пройти немало времени, прежде чем такие жалобы начнут поступать и прежде чем мы как сообщество сможем что-то с этим сделать.

В то же время, если мы сможем использовать эти широкие наборы данных по DNS, которые предполагается использовать в рамках инициативы DAAR для информирования сообщества, тогда, возможно, мы сможем обнаруживать проблемы заблаговременно, а не просто ждать, пока не поступит жалоба на то или иное конкретное нарушение, от которого к тому времени уже наверняка пострадает множество жертв.

А вот второй регистратор, AlpNames, который еще работает. То же самое, очень высокий уровень злоупотреблений. Кроме

того, в то же время, когда проводилось исследование группой по анализу конкуренции, потребительского доверия и потребительского выбора, этот конкретный регистратор предлагал массовую регистрацию имен, когда владелец домена мог перейти на сайт AlpNames и зарегистрировать 2000 доменных имен за раз, при этом AlpNames помогали им создавать домены, они предлагали пользователям специальный алгоритм для автоматического формирования доменных имен. То есть можно было создать 2000 случайных доменных имен, возможно даже, я уверен, в законных целях, и зарегистрировать эти домены. Так что не удивительно, что по этому регистратору отмечались высокие уровни злоупотреблений, однако не поступало никаких жалоб, на основе которых можно было бы действовать. То есть процедура приостановки работы им не угрожала.

И вот это, все эти массовые данные и то понимание, которое нам удалось из этого извлечь, говорит о том, что сообщество имеет дело в возможным пробелом в политиках.

Кажется, я тут все время не ту кнопку нажимаю, или я просто хочу постоянно выделять этих двух регистраторов.

[Смех]

Так что то, к чему мы пришли… например, группа по анализу конкуренции, потребительского доверия и потребительского выбора смогла использовать эти данные и выработать

конкретные рекомендации в отношении политики, которые будут обнародованы в нашем проекте устава по злоупотреблениям DNS, который будет выпущен в ближайшие неделю-две. Но, понимаете, это не должно закончиться на группе по анализу конкуренции, потребительского доверия и потребительского выбора . Вместо этого мы как сообщество, по мере того, как у нас будет все больше и больше таких данных, доступных и прозрачных для сообщества, неважно, в рамках системы DAAR или через членов сообщества специалистов по обеспечению кибербезопасности, таких как антифишинговая рабочая группа, фонд Secure Domain Foundation, Spamhaus, Stopbad, когда все эти члены предлагают и представляют эти данные, мы как сообщество должны не просто использовать их для блокировки имен на уровне операций, вместо этого их следует использовать в качестве информационной основы для принятия решений в отношении политик, для обнаружения таких пробелов, чтобы мы действительно могли перейти от модели, предполагающей реагирование на нарушения, к некой проактивной модели, в рамках которой регистраторы и операторы регистратур затрудняли бы повторное злоупотребление их услугами со стороны злоумышленников, а также чтобы мы могли использовать эти данные для измерения прогресса и понимания того, удается ли нам на самом деле противодействовать злоупотреблениям в рамках какого-то комплексного подхода. И я также надеюсь,

что эта комиссия сегодня сможет на самом деле обсудить это с разных точек зрения, потому что, конечно же, это затрагивает самые разные области в сообществе, поэтому нам нужно сделать это правильно.

Раз уж сейчас у нас есть данные, которые можно использовать и принимать решения на их основе, то мы должны действительно их использовать и разрабатывать на их основе политики, которые позволят нам создать более совершенную DNS для всех нас. На этом я возвращаю эстафетную палочку Кэтрин.

ИРАНГА КАХАНГАМА: Спасибо, Дэвид и Дрю, за ваши презентации. Я хочу еще раз подчеркнуть, что на ответы на вопросы выделяется по две минуты максимум. Мы уже на пару минут запаздываем, однако я хочу по крайней мере предоставить слово как можно большему количеству участников.

Итак, еще раз, я начну вопросы с некоторых… с членов комиссии, а затем, после их ответов, присутствующие в аудитории приглашаются к микрофонам и к участию в этой дискуссии.

Так что начнем, пожалуй, с Алана, если он не против положить начало этой дискуссии. Возможно, стоит начать с верхушки… так сказать, цепочки.

Мы только что слышали, что Дрю говорил о некоторых примерах. Когда у нас есть очевидный нарушитель, какие инструменты имеются в распоряжении регистратуры, чтобы как-то преобразовать эти данные о наблюдаемых тенденциях в данные о регулярных нарушителях или злоумышленниках, чтобы можно было определить какие-то из этих проблем?

АЛАН ВУДС (ALAN WOODS): Спасибо, Иранга. Алан Вудс. Просто представлюсь. Я представляю регистратуру Donuts. Если перейти прямо к вопросу, то есть, вы сказали «очевидный нарушитель», и я сразу вздрогнул, потому что, к сожалению... знаете, я вижу данные и мы видим данные, которые поступают в такие системы, как DAAR. Они поступают от этих источников, которые дают нам просто фантастически полезные списки потенциальных нарушителей.

Однако мы сейчас не в том положении, чтобы сказать, что кто-то является очевидным нарушителем, потому что, к сожалению, у нас по-прежнему нет доказательств, которые могли бы лечь в основу такого вывода, на основе которых можно было бы предпринимать какие-то действия или повышать уровень этого вопроса, передавать его регистратору или соответствующим инстанциям на рассмотрение.

Так что первый вопрос, который нам на самом деле нужно задавать, это как мы будем знать, что это очевидное нарушение? Я хочу сказать, что мы действительно используем… разумеется, когда у нас действительно есть информация и доказательства, то, разумеется, тогда мы эти доказательства используем. Мы их соберем, мы их объективно рассмотрим, а затем мы передадим их на следующий уровень, тому, кто должен этим заниматься, то есть в данном случае, наверное, это был бы соответствующий регистратор.

И тогда… если этот регистратор не предпримет никаких действий, ну, тогда, очевидно, регистратура сама предпримет… ну или рассмотрит возможность предпринять такие действия.

То есть на данный момент те инструменты, которыми мы располагаем, да, они позволяют нам учитывать какие-то индикаторы, которые мы получаем через такие списки, как, скажем, Spamhaus или SURBL. Однако после этого мы должны сами найти дополнительную информацию, дополнительные доказательства, чтобы закрыть этот пробел между статистическими показателями и доказательствами, которые можно использовать в деле. И я передаю слово дальше.

ИРАНГА КАХАНГАМА: Спасибо, Алан. Я хочу только кратко продолжить, как вы считаете, можно сказать, что эти статистические данные как минимум неплохо подходят, чтобы определить то, что может потребовать дополнительного изучения, так сказать, в помощь регистратуре?

АЛАН ВУДС: Да. И, на мой взгляд, это несколько противоречиво, но да, можно сказать, что это может указывать в этом направлении. Однако во многих случаях единственное другое доказательство, которое мы можем найти при анализе, это то, что данный домен включен в блок-лист. Так что мы бы хотели иметь возможность получать эти дополнительные детали или дополнительные способы выяснить, почему этот домен был включен в список, а не просто констатацию факта такого включения.

То есть это... для нас это трудно. В таких случаях мы делаем все, что можем. Если мы видим, что что-то отмечено, мы делаем все, что в наших силах, чтобы попытаться определить причину, по которой это было отмечено. Однако это не всегда очевидно. И получить такую информацию очень трудно, особенно от тех поставщиков блок-листов, которые не предоставляют нам такую информацию, потому что не могут или потому что у них ее нет или потому что это их коммерческая тайна.

КЭТРИН БАУЭР-БУЛЬСТ: Дэвид, вы хотите вкратце к этому вернуться?

ДЭВИД КОНРАД: Просто добавить, что одна из причин, по которым в системе DAAR хранятся исторические данные, это чтобы помочь в определении тенденций за длительные периоды времени, поэтому включается информация о нарушениях за длительные периоды времени. Так что я на 100% согласен с тем, что, так сказать, сама идея о том, что какие-то нарушения могут быть очевидными, — знаете, это, скорее всего, субъективно, а на самом деле нужна дополнительная информация, чтобы отличить настоящих злоумышленников от, к примеру, кого-то, у кого… кому нравится регистрировать случайные строки в качестве доменных имен.

Однако отчасти эти усилия, которые мы пытаемся реализовать в сообществе, заключаются в предоставлении информации, в особенности за длительное время… за длительные периоды, чтобы в рамках обсуждения политик можно было четко определять тенденции злоупотреблений в тех или иных областях пространства имен.

ИРАНГА КАХАНГАМА: Спасибо.

Затем у нас выступит Род, а потом мы видим микрофон 2.

РОД РАСМУССЕН: Здравствуйте. Род Расмуссен. Для протокола: я сейчас говорю от себя лично, а не как представитель SSAC.

Я хочу прямо ответить на этот вопрос, потому что, на мой взгляд, тот ответ, который мы услышали, касается того, как та или иная конкретная организация определяет нарушения надежным способом, а не как вообще определить нарушения надежным способом. Последнее требует наличия политики, доверия и т. п.

Есть определенные… эта отрасль существует уже 10 или 15 лет, в ней сложились чрезвычайно надежные способы определения систематических нарушений.

Затем эти вещи переходят в браузерные технологии, такие как Internet Explorer или Google Safe Browsing, или в службы электронной почты, такие как Gmail или Hotmail, и т. п. Эти правила автоматически переходят в это все миллионами в день, в считанные секунды после обнаружения.

То есть что касается определения, то здесь технология очень надежна. Было найдено множество способов добавлять что-то в белые списки и сводить ложные срабатывания практически к нулю. То есть такая технология существует.

Что… ключевой момент здесь — это как преобразовать это… эту информацию в конкретные действия. А для этого нужны договора. Для этого нужно доверие. Для этого нужно еще много чего, что должно быть организовано в виде единого

концептуального решения для этой задачи, чтобы можно было предпринимать необходимые действия в различных областях, идет ли речь о регистратуре доменов, о регистраторе, поставщике услуг электронной почты или о поставщике веб-приложений.

То есть я просто хотел ответить, что в том, что касается технологий, эта проблема решена. Это не значит, что она решена с точки зрения политик. Спасибо.

ИРАНГА КАХАНГАМА: Спасибо, Род.

Можно теперь перейти к микрофону?

ДЕЙВ ПИШИТЕЛЛО (DAVE PISCITELLO): Дейв Пишителло из ICANN. Мне не нравится фраза «очевидные нарушения». Это точно не то, что мы измеряем в системе DAAR. В системе DAAR измеряем это угрозы безопасности, то, что мы считаем нарушениями, основываясь при этом на блок-листах и репутационных списках. А это, на мой взгляд, отчетливо отличается от обязательства, согласно которому регистратура, или регистратор, или компания, осуществляющая хостинг DNS, или интернет-провайдер должны взяться за ту информацию, которая им была представлена, провести свое расследование и подтвердить то, что было заявлено.

Если бы я находился в таком положении, я бы попытался получить какое-то сообщение электронной почты, так сказать, с URL-адресом, или какое-то вложение, которое содержало бы URL-адрес, или перейти на веб-сайт, воспользоваться утилитами WebGet или curl, что-то такое нестрашное. Существует множество процедур, которые можно ожидать в рамках комплексной проверки и аудита на уровне регистратор-регистратура. Я не утверждаю, что это не связано с затратами.

Но система DAAR не предназначена выступать в роли некой инстанции, в которую можно обратиться и получить полный ответ. Система DAAR задумана как механизм своего рода переписи всех ресурсов во всем пространстве имен, на всем ландшафте угроз, чтобы попытаться получить какие-то цифры, с помощью которых мы могли бы определять, что вот здесь политика работает хорошо, здесь политика работает плохо, и как-то сводить это все воедино.

КЭТРИН БАУЭР-БУЛЬСТ: Спасибо, Дейв.

Грэм, позвольте мне подбросить эту тему регистратору. Мы сейчас в нашей дискуссии дошли до вопроса о том, как далеко простирается охват тех индикаторов, которые у нас есть. Итак, у нас есть система DAAR, которая предоставляет нам базовые данные для оценки, и еще мы услышали, что нужно сделать

что-то еще на стороне регистратур и регистраторов, чтобы эта информация могла стать основой для инструментов, которые позволяли бы предпринимать какие-то действия против тех клиентов, которые, возможно, не соблюдают ваши условия и положения.

В таком случае, конечно, в фокусе внимания оказываются эти самые условия и положения, и мы переходим к тому, что нам необходимо, чтобы иметь возможность предпринимать действия в рамках этих условий и положений, а также как на это можно влиять в контексте организации вашей политики. Могу я попросить вас сказать пару слов об этом?

ГРЭМ БАНТОН (GRAEME BUNTON): Разумеется. Спасибо, Кэтрин. Это Грэм Бантон из компании Tucows.

Там есть несколько моментов, которые мне кажутся интересными, хотя Алан поднял важный вопрос. Как вы только что сказали, связать этот блок-лист с фактическими доказательствами, на основании которых можно было бы предпринимать какие-то действия, — задача нетривиальная.

И я считаю, к тому, о чем только что говорил Дэйв, что... так сказать, методы, которые можно использовать для борьбы с нарушениями на вашей платформе, это как бы изначально предполагает определенный уровень сложности и компетентности с вашей стороны в том, что касается

персонала, занимающегося мониторингом актуальной очереди угроз, а это, честно говоря, не каждому регистратору на этой планете доступно. Конечно, когда осуществляется оптимизация очереди нарушений с приоритетом скорости и объемов передачи данных, у вас может и не быть времени как-то глубоко в этом разбираться.

Есть еще один момент, который я хотел бы затронуть, потому что я часто слышу, как об этом говорят. Мы были свидетелями того, как автоматически формируемые доменные имена использовались для управления сетями. То есть это не обязательно что-то плохое. Кое-где такой подход используют для организации работы бизнеса.

Чрезвычайно трудно отследить повторяющиеся действия злоумышленников, основываясь на тех данных, которые поступают вам в очередь сообщений о нарушениях, а также на ваш мониторинг.

Нет какого-то простого ответа, который однозначно приходил бы в голову, хотя мы были бы очень заинтересованы в этом, потому что это позволило бы снизить количество нарушений на нашей платформе, а это именно то, в чем мы очень заинтересованы. Однако это потребовало бы очень широкой перспективы картины данных, которые поступают в очередь сообщений о нарушениях, а этого очень непросто достичь.

КЭТРИН БАУЭР-БУЛЬСТ: Спасибо, Грэм. Кажется, Алан тоже хотел что-то сказать.

АЛАН ВУДС: Это снова Алан Вудс. На самом я только хотел сказать, что то, что Дэйв... то, что сказал перед этим Дэйв Пишителло, я только хотел сказать, что если бы он был ближе ко мне, я бы просто встал и пожал ему руку, потому что для меня это... очень важно об этом заявить. А именно что DAAR — это проект отображения статистических данных, однако работа на уровне между DAAR и фактическими действиями должна выполняться регистратором или регистратурой, или еще какой-то стороной. Так что спасибо, Дейв.

ИРАНГА КАХАНГАМА: Спасибо, Алан.

Давайте быстро перейдем к чему-то чуть более конкретному, Род, вы говорили, что многое из этого уже как бы сделано. Не могли бы вы немного конкретнее рассказать, какого рода данные нужны для того, чтобы сделать возможными такого рода действия?

РОД РАСМУССЕН: Разумеется. Существует множество разнообразных методик. Это, конечно, зависит от типа нарушений. То есть, к примеру, на самом деле легко обнаруживаются такие вещи, как работа алгоритмов создания доменных имен. Алгоритмы создания

доменных имен используются вредоносным ПО для формирования последовательности доменных имен, которые потенциально могут быть зарегистрированы в будущем. То есть если разобрать такое вредоносное ПО методом обратного инжиниринга, можно получить список доменных имен, которые потенциально могут использоваться. Затем можно отслеживать регистрацию таких доменов и действовать соответственно ситуации, потому что это не обязательно действия злоумышленников, это могут быть какие-то исследователи в области безопасности. Это один способ.

Очевидный способ — это спам, он используется уже больше десяти лет, больше 15, больше 20 лет, наверное, если говорить о таком базовом, рудиментарном анализе. А вот уже как это анализировать — это может быть очень сложно.

Различные платформы, Facebook, социальные сети — они все это используют. Программы для работы с электронное почтой… или платформы электронной почты — они все проверяют содержимое, когда пользователи разрешают им его проверять, это делается очень массово, и при этом анализируются домены, в тех случаях, если это те домены, которые их интересуют.

И исходя из этого вы, пожалуй, сделаете что-то с этой информацией, чтобы как-то сопоставить ее с какими-то

метаданными, которые вы, возможно, получаете, скажем, через запрос WHOIS или запрос к системе DNS, или через выборку из вашей собственной базы данных известных или неизвестных объектов. Существуют целые наборы различных формул, которые можно для этого использовать.

А еще есть инструменты, которые пристраиваются к веб-браузерам, существуют сетевые устройства безопасности, которые анализируют входящий или исходящий трафик в сетях и сопоставляют… существуют очень сложные и совершенные алгоритмы машинного обучения для обнаружения таких вещей, как туннелирование и прочие действия для управления сигналами и мониторинга ваших сетей. Существует широчайший спектр технологий, которые могут совместно использоваться для формирования списков по таким разным областям нарушений.

ИРАНГА КАХАНГАМА: Спасибо. Кажется, вы могли бы говорить об этом весь день. Думаю, стало ясно одно: ключевым фактором в этой области является разнообразие доступных данных. Кажется, у нас есть вопрос от удаленного участника. Мы будем принимать вопросы удаленных участников позже, это нужно как-то решить. Кэтрин, хотите задать следующий вопрос?

КЭТРИН БАУЭР-БУЛЬСТ: Да. Я на самом деле хочу вернуться к этому… к разным типам данных, которые нам нужны для использования в качестве информационной основы принятия решений, о чем так красноречиво говорил Дрю, эта идея о наблюдении общих тенденций и событий, которые могут использоваться в качестве информационной основы принятия решений, с последующим переходом к более конкретной информации, которую должны видеть регистратуры и регистраторы, чтобы иметь возможность предпринимать конкретные действия в каждом отдельном случае, что может потребовать данных иного качества. Это, конечно, не то же самое, что уголовное расследование или что-то такое. Это, разумеется, также может зависеть от конкретных условий и положений того или иного поставщика услуг.

Я бы хотела, пожалуй, перейти к Дениз, которая обладает специфическим опытом в формировании стандартов для сообществ и для пользователей. Если исходить из вашего опыта, можно ли из него извлечь урок о том, каким образом нужно составлять условия и положения, чтобы обеспечить возможность эффективного реагирования на нарушения?

ДЕНИЗ МИШЕЛЬ: Это Дениз.

Итак, у нас есть широкая глобальная система обеспечения безопасности и недопущения нарушений на всех наших

платформах, которая постоянно обновляется и отслеживается.

И мы осуществляем широкую координацию между разными отраслями и секторами для обмена опытом и практическими методиками, как в том, что касается обслуживания, так также и в том, что касается обмена данными в целях безопасности.

Я думаю… если говорить о разнице между тем, что делаем мы и что делается в каких-то областях на уровне регистраторов и регистратур, то одним из элементов, которые еще должным образом не решены, остается вопрос поощрения и мотивации.

Группа интересов коммерческих пользователей представила обширные комментарии к исследованию нарушений, проведенному группой CCT, и предложила ряд очень конкретных вариантов использования результатов этого исследования в качестве исходной точки для расширения наших коллективных возможностей противодействовать нарушениям и усовершенствовать наши усилия в целом. Это такие вещи, как привязка поощрения к использованию практических мер противодействия нарушениям, анализ взносов, которые должны платить регистраторы и регистратуры, и привязка их к использованию определенных практическим методик и результатам, обеспечение того… это первое исследование злоупотреблений, но мы должны проводить их регулярно, чтобы иметь точные данные о

тенденциях, на основе которых можно было бы принимать какие-том меры, чтобы мы ужесточили проверку соблюдения норм и правил для регистратур с высоким уровнем нарушений.

Много чего можно сделать прямо сейчас, чтобы иметь возможность действовать на основании таких данных о нарушениях. И чем раньше мы запустим в работу инициативу открытых данных и передадим ее в открытое пользование, и чем раньше мы увидим отчет DAAR в бета-формате на веб-сайте, тем быстрее мы сможем это сделать. Спасибо.

КЭТРИН БАУЭР-БУЛЬСТ: Передаем слово аудитории. Это первый вопрос.

РЕДЖ ЛЕВИ (REG LEVY): Спасибо. Это Редж Леви из Tucows и ENOM. Я хочу коснуться того, что кто-то недавно сказал об условиях и положениях. Совершенно верно, что у большинства из нас есть условия и положения, в которых сказано, что мы можем закрывать ресурсы по любым причинам или вообще без причин, просто потому, что нам так хочется. Однако мы используем их для защиты наших интересов, а не для выполнения полицейского надзора за Интернетом или какого-либо мониторинга. Они используются на случай возникновения ситуаций, о которых не было известно заранее, но в которых будет совершенно необходимо действовать в момент их возникновения, чтобы в

таких случаях у нас были юридические права для таких действий. Они существуют не для того, чтобы мы действительно могли делать все, что нам заблагорассудится.

КЭТРИН БАУЭР-БУЛЬСТ: Если говорить о... думаю, через минутку мы перейдем к следующему разделу. Но я хочу задать Джонатану один последний вопрос об одном моменте, который поднимался в ходе презентации этой идеи определенных индикаторов.

Вот Дрю сказал, что есть конкретные виды нарушений, которые мы отслеживаем, и есть разные способы распространения. Один из них, как он сказал, — это спам. А еще один, который он отметил, — это то, что иногда нарушения прав на интеллектуальную собственность могут быть связаны со злоупотреблениями или могут служить индикаторами возможных нарушений. Есть ли... можно ли говорить об этих индикаторах и пользе от них в том, что касается обнаружения нарушений?

ДЖОНАТАН МАТКОВСКИЙ: Разумеется. Это Джонатан Матковский из компании RiskIQ, член группы интересов по вопросам защиты интеллектуальной собственности, в данном случае я выступаю от своего имени.

Во-первых, что касается обязательств регистратора согласно соглашению об администрировании домена верхнего уровня… согласно соглашению об аккредитации регистратора в части реагирования на сообщения о нарушениях и должного их расследования, то это на благо сообщества. Так что я бы призвал всех этим пользоваться и использовать эту возможность, чтобы мы как сообщество были защищены от нарушений. И это касается любых незаконных действий.

Мы можем согласиться в том, что фишинг… когда с помощью приманки у пользователя похищаются личные данные, это имеет прямое отношение к содержанию.

Мы слышали то, что в отчете SADAG говорилось об использовании злоумышленниками тайпсквоттинга и соответствующих доменов. Справедливо, причем во многих разных аспектах, и то, что интеллектуальная собственность… и содержание имеют отношение к угрозам, к угрозам безопасности. В особенности к, так сказать, сложным угрозам, когда используется сразу несколько разных адресов в Интернете.

И я уверен, что все читали о том, как всплывающие окна Adobe Flash использовались для того, чтобы побудить пользователей загружать вредоносное ПО или ПО,

использующее вычислительные мощности компьютера пользователя.

Так что взаимосвязь определенно существует. И я бы также сказал, что операторы регистратур не всегда могут видеть, что происходит на уровне регистраторов, не реагирующих на сообщения о нарушениях. То есть нужно, чтобы они получали уведомления в тех случаях, когда регистратор не… не выполняет свои обязательства, чтобы они могли принимать меры.

Эта информация должна включаться в данные технического и статистического анализа, в тот набор данных, который передается в ICANN. И ICANN может запрашивать эти данные в любой момент.

Так что я бы сказал, что исследование DAAR, проект DAAR заслуживает внутреннего использования. Я бы рекомендовал отделу соблюдения договорных обязательств ICANN использовать его для своего внутреннего аудита и ситуационных проверок. Если вернуться и посмотреть на… на некоторые из наборов данных, которые я видел по крайней мере в отчете SADAG, можно видеть, как, даже несмотря на то, что было подано меньше сообщений о нарушении обязательств, если говорить относительно, в сравнении с сообщениями о нарушениях… знаете, там Nanjing и все остальные.

Посмотрите, к примеру, на Dynamic Dolphins, и вы поймете, что произошло. Просто посмотрите на ICANN, и вы поймете, что произошло в 2013 году.

Вот. Спасибо.

ИРАНГА КАХАНГАМА: Спасибо, Джонатан. А наша дискуссия переходит к следующему слайду. Спасибо. Хочу только напомнить, как создать эффективную и прозрачную систему сообщения о нарушениях.

Я думаю, для нашего первого вопроса я предоставлю слово Татьяне, которая будет говорить о докладе Дэвида Конрада, в котором упоминались различные случаи, в которых эти блок-листы используются в разных браузерах и системах электронной почты, которые в конечном итоге также использовались, так сказать, некоммерческими пользователями.

Так что, пожалуй, мой вопрос к вам будет звучать так: в чем интересы конечных пользователей пересекаются с какими-то данными этого статистического анализа? И могут ли данные о злоупотреблениях DNS эффективно использоваться и применяться для создания каких-то удобных для пользователей инструментов, с помощью которых можно было бы информировать широкую публику о рисках и возможных источниках угрозы в Интернете?

Татьяна?

ТАТЬЯНА ТРОПИНА: Большое спасибо. Это Татьяна Тропина.

Прежде всего я бы хотела разрешить одно недоразумение. Я не думаю, что мы представляем конечных пользователей. Мы представляем некоммерческих пользователей, здесь есть большая разница, потому что пользователи могут быть коммерческими и некоммерческими.

Однако я хочу сказать, что у нас действительно есть своя позиция в том, что касается всей проблемы создания инструментов и систем сообщения о нарушениях.

Я хочу еще раз подчеркнуть, что мы — это группа интересов некоммерческих пользователей. То есть, мы на самом деле не собираем статистические данные, понимаете? Мы не приостанавливаем работы веб-сайтов. Однако если говорить о том, что мы поддерживаем — какой инструмент будет использоваться?

Если говорить обо мне лично, то я точно могу сказать, что я за сбор статистики. Я за обмен информацией и за информирование отрасли.

Однако здесь, в ICANN, мы поддерживаем четкое разделение технических аспектов злоупотреблений DNS, которые относятся к миссии ICANN, и о нарушениях, связанных исключительно с содержанием. Потому что не все, что может противоречить тем или иным законам, относится к техническим аспектам злоупотреблений DNS.

И мы полагаем, что ICANN и те инструменты, которые ICANN использует, должны соответствовать миссии ICANN. Я знаю, что кто-то может принести сюда свое соглашение об аккредитации регистратора. Однако соглашение об аккредитации регистратора было составлено в 2013 году, а миссия ICANN была определена в переходной период. Поэтому я считаю, что это в данном случае важнее.

А во-вторых, мы должны быть осторожны. Я уже много говорила о предупредительных подходах. Где проходит эта граница между действиями, реагированием и упреждающими ударами. Что означает «предотвращать»? Когда… когда отраслевые игроки должны принимать меры? Понимаете? Что означает «предотвращение»? И я считаю, что нам нужно придерживаться ясности. Я уже говорила, что нам нужно очень узкое определение злоупотреблений DNS. Кроме того, мы как некоммерческие пользователи считаем, что нам нельзя забывать о том, что главное, когда речь идет о нарушениях, — это не только приостановить работу веб-сайта, но и поймать тех, кто нарушает закон и осуществляет такие злоупотребления. А это работа правоохранительных органов. Извините. Мы займем еще 20 секунд.

То есть мы не хотим, чтобы какие-то посредники или представители отрасли выступали в роли полиции контента, или вообще в роли полиции в любом смысле.

Поэтому нас пугает, когда мы слышим такие фразы, что отрасль должна выполнять функции полиции. Не должна. Она должна так или иначе заниматься злоупотреблениями DNS. Спасибо.

КЭТРИН БАУЭР-БУЛЬСТ: Спасибо, Татьяна.

Сейчас я перейду к Дрю и спрошу, что вы думаете как исследователь проблем безопасности о том, как часто эти данные следует публиковать, чтобы они были полезны. Можно ли говорить о какой-то минимальной или идеальной периодичности, с вашей точки зрения, чтобы эти данные могли использоваться сообществом специалистов по обеспечению безопасности?

ДРЮ БЭГЛИ: Спасибо. Я считаю, если мы посмотрим на то исследование, проведенное по поручению группы CCT, на которое я уже ссылался ранее, то я считаю, что очень важно, чтобы это не было что-то, что просто выходит раз в пять лет, и каждый раз какая-то группа по анализу рассматривает это или, к примеру, какие-то другие группы по анализу, потому что я знаю, что эта тематика находится на пересечении сфер интересов разных групп по анализу. Вместо этого я считаю, что было бы очень полезно, возможно, если система DAAR будет выдавать сообществу какую-то прозрачную статистику, возможно,

чтобы это был какой-то постоянно обновляемый набор данных в той или иной форме. И тогда можно было бы проводить периодический анализ того, что эти данные на самом деле означают. То есть данные были бы в распоряжении сообщества и их можно было бы разбивать и анализировать. И тогда, возможно, можно было бы проводить какой-то всесторонний комплексный анализ, как это было сделано в рамках исследования, проводимого по поручению группы CCT. Дважды в год, например. Мне кажется, это было бы очень полезно.

Потому что очень важно, чтобы мы понимали тенденции, чтобы подход был ориентирован на перспективу. Потому что определенные фишинговые кампании или другие кампании, связанные с вредоносным ПО, могут приводить к искажению результатов в отдельных кварталах. Поэтому очень важно проводить постоянные, текущие исследования, чтобы понимать, где мы находимся как сообщество.

Если вы не возражаете, я бы хотел немного ответить на замечания Татьяны. Потому что я считаю, что Татьяна сделала ряд важных замечаний, которые действительно отражают разнообразие нашего сообщества и точек зрения по данному вопросу.

И именно поэтому я считаю, что очень важно то, что я подчеркнул на одном из моих первых слайдов, чтобы вместо

того, чтобы, так сказать, провести годы, обсуждая все, что может считаться нарушением в одной стране и не считаться в другой и т. д. и т. п., очень важно, чтобы мы как сообщество начали с тех вопросов, по которым у нас есть консенсус и для решения которых у нас на самом деле уже есть полномочия в виде запрета на те или иные виды деятельности в соглашениях, чтобы мы могли начать с этих очень технических моментов, вместо того, чтобы, так сказать, блуждать в потемках.

Так что я считаю, что для нас важно отталкиваться от того, что сказала Татьяна в этом отношении. И я также считаю, что Алан поднял очень важный вопрос о том, насколько трудно работать, когда мы рассматриваем проблемы, реагируя на них постфактум, когда мы следуем за злоумышленниками. Потому что для этого, конечно же, нужны доказательства.

Кроме того, как указала Татьяна, провайдер — это не правоохранительные органы. То есть это разные вещи — приостановить работу каких-то доменов за нарушение условий обслуживания и сделать что-то в свете потенциально преступного характера каких-то действий.

Поэтому я действительно считаю важным, чтобы мы перешли к какой-то проактивной модели, в рамках которой мы могли бы использовать очевидные индикаторы, возможно, подождать, пока домен не начнет работать, если было что-то

подозрительное в самой регистрации. Возможно, он не начнет работать через пять минут. Возможно, его нужно будет проверить вручную и это займет 24 часа, прежде чем вы позволите использовать этот домен, или что-то такое. Я хочу сказать, что в отношении разных поставщиков услуг могут работать разные модели, однако, на мой взгляд, важно, чтобы мы перешли на такую модель.

ИРАНГА КАХАНГАМА: Спасибо, Дрю.

Дэйв, вы хотели дополнить?

ДЭВИД КОНРАД: Да. Просто о тех планах, которые существуют на данный момент в отношении публикации тех данных, которые мы формируем в системе DAAR, чтобы формировать какой-то ежемесячный отчет, какие-то документы по тем статистическим данным, которые мы видим на уровне сводных данных по регистратурам и регистраторам.

И эта информация была бы… затем планируется со временем обнародовать эти данные в рамках инициативы открытых данных, чтобы можно было на основании собираемых нами данных проводить анализ изменения тенденций за периоды времени.

Однако это то, что пока планируется. И мы на самом деле очень заинтересованы в любых мнениях и предложениях, которые могут быть у сообщества в отношении периодичности публикации таких данных или, так сказать, методики публикации таких данных.

ИРАНГА КАХАНГАМА: Только… извините, в двух словах, у вас намечена какая-то дата, когда можно будет увидеть первый отчет?

ДЭВИД КОНРАД: В настоящее время мы на самом деле проводим своего рода оценку лицензионных требований, которые у нас есть по разным каналам предоставляемых, то есть получаемых нами данных.

Так что у меня не очень получается сейчас сказать вам точную дату. Потому что… юристы.

[Смех]

ИРАНГА КАХАНГАМА: Справедливо. Теперь мы можем перейти к микрофонам. Номер 3, пожалуйста.

МИЛТОН МЮЛЛЕР (MILTON MUELLER): Это Милтон Мюллер, Технологический институт Джорджии. Когда мы говорим о DAAR, кажется, есть два разных подхода. Когда я слушаю то, что говорит об этом Дэвид, я слышу, что мы собираем множество данных, публикуем отчеты, а затем эти отчеты можно использовать в качестве информационной основы для разработки политик. Однако я слышал, что регистраторы и регистратуры подчеркивают, что между тем, чтобы получить эти данные, и тем, чтобы иметь возможность предпринять какие-то действия, нужно проделать еще много разной работы.

С другой стороны, я слышу, как кто-то говорит о каких-то более упреждающих действиях, чтобы на основе этих данных предпринимать какого-то рода упреждающие действия.

Так что в этом контексте у меня есть вопрос о том, чем именно является или будет являться система DAAR. Насколько она будет расширяемой, Дэвид? Угрозы меняются. Сейчас вы полностью полагаетесь на сторонние репутационные списки. Вы же сами их не формируете? ICANN на самом деле не собирает данные, на которых эти списки основываются. Вы просто составляете их из других списков и используете как ресурс для отрасли DNS, что, на мой взгляд, прекрасно.

Но угрозы меняются. Преступники меняются. Их приемы меняются.

И как вы будете реагировать на развитие этих новых технологий? Вы работаете над развитием потенциала для этого, или собираетесь и дальше полагаться в получении этих данных на сторонних поставщиков?

ДЭВИД КОНРАД: Простой ответ таков: мы делаем то, что нам говорит сообщество.

Если, в контексте системы DAAR, отслеживаемые нами обнаруженные угрозы относятся к угрозам, определенным в Пекинском коммюнике GAC. Если на каком-то этапе сообщество предложит нам отслеживать какие-то другие формы нарушений, тогда мы посмотрим, что мы сможем сделать для того, чтобы включить их в структуру DAAR. Она расширяемая.

Что касается источников данных, то основное требование к используемым нами источникам данных — они должны быть общедоступными. Если, к примеру, существует какой-то источник данных, который формируется ICANN и который мы делаем доступным в рамках инициативы открытых данных или какого-либо другого механизма, тогда мы можем включить его в систему DAAR. Но, опять же, это будет зависеть от того, что будет требовать от нас сообщество.

И я думаю, что мой коллега, г-н Пишителло, тоже может кое-что добавить по этой теме.

ДЕЙВ ПИШИТЕЛЛО: Да, немного. Я на самом деле рад, что вы задали этот вопрос, потому что, я думаю, через год мы сможем сделать кое-то такое, чего мы еще никогда не могли делать в истории нашей отрасли. У нас будет история за полтора года. А когда у вас есть полтора года истории, то вы можете сделать многое, в т. ч. вы можете рассмотреть тенденции массовых действий и миграции. Вы можете проанализировать задержку или временной интервал между резким росток количества регистраций по той или иной регистратуре или регистратору, а также то, как эти имена используются. То есть я могу показать вам график, если бы я мог показать вам график, на котором видно, что по тому или иному регистратору был резкий рост на примерно тысячу регистраций, а затем эти зарегистрированные имена на самом деле выдавались постепенно за какой-то период курирования. Тогда это совсем не то же самое, что и… некоторые из тех измерений, на основе которых в отчете SADAG был проведен анализ скомпрометированных доменов и доменов, регистрируемых с незаконными целями. То есть для нас это что-то новое, что тоже надо рассмотреть.

Что касается эволюции угроз, то, вы знаете, я говорил с теми, кто… с разработчиками системы, в которой используются списки загрузки, или черные списки. Списки загрузки или черные списки — это списки, которые используются на сайтах для борьбы с распределенными атаками типа «отказ в

обслуживании». Это новая угроза. Если мы будем чувствовать, что… что данные в этой базе данных заслуживают доверия, надежны, точны, общедоступны, то есть отвечают всем нашим критериям, тогда нам нужно будет сесть и подумать, не хотим ли мы внедрить это в нашу систему, потому что сообществу было бы полезно знать, что вот есть такая новая угроза. Однако, опять же, как уже сказал Дэвид, знаете, мы… мы построили платформу, которая, на мой взгляд, отличается очень и очень большой расширяемостью во многих направлениях, и если мы… если мы понимаем, какие угрозы мы хотим измерять и что мы будем использовать с такими измерениями, то я считаю, что мы можем сделать многое из того, что вы предлагаете.

ДЭВИД КОНРАД: Спасибо, Дейв. Кажется, у нас есть два вопроса от удаленных участников. Пожалуй, я попрошу вас зачитать оба эти вопроса, и мы на них ответим, а затем, думаю, мы перейдем к последней трети из наших тем для обсуждения.

ДЖЕЙМС КОУЛ (JAMES COLE): У нас есть вопрос от Максима Альзобы из Фонда содействия развитию технологий и инфраструктуры Интернета (FAITID). «Планирует ли офис технического директора ICANN как-то взаимодействовать с группой заинтересованных сторон-регистратур и группой

заинтересованных сторон-регистраторов по вопросам инструментов DAAR, чтобы эта часть сообщества, то есть регистратуры и регистраторы, также могли пользоваться преимуществами этого ресурса?».

ИРАНГА КАХАНГАМА: Пожалуйста, прочитайте и второй тоже. Извините.

ДЖЕЙМС КОУЛ: Второй вопрос таков: «По какой причине в качестве надежного источника данных используется компания с такой небезупречной практикой, как Spamhaus? Процедура передачи разрешения проблем на более высокий уровень этой компании подразумевает отключение владельцев доменов, регистраторов и Интернета, блокирование почтовых серверов регистратора и DNS-серверов без какой бы то ни было подотчетности или прозрачности перед сообществом».

ДЭВИД КОНРАД: Спасибо за эти вопросы. Знаете, я отвечу сначала на последний вопрос... мы используем Spamhaus, потому что в сообществе специалистов по борьбе с нарушениями Spamhaus считается... заслуживающим доверия и надежным источником и отвечает всем критериям, которые мы указали в первоначальном таком пробном проекте процедуры выбора

поставщиков блок-листов. Также следует отметить, что независимо от, так сказать, того, что мы можем думать о том или ином конкретном блок-листе, реальность такова, что эти блок-листы используются в нашей отрасли, в секторе науки и образования, коммерческими и некоммерческими поставщиками для организации трафика в Интернете, так что, знаете, если мы будем притворяться, что тот или иной блок-лист нам не подходит, потому что так случилось, что вы не согласны с их политиками, это не отменит того факта, что другие полагаются на этот блок-лист для блокировки трафика от определенных доменов или IP-адресов. Если критерии будут изменены и Spamhaus перестанет считаться достойной альтернативой или полезным поставщиков данных для нас, тогда, конечно, мы сможем подстроиться. И, знаете, если вы можете продемонстрировать какие-то доказательства того, что они не соблюдают свои собственные спецификации в отношении процедуры обработки запросов, то это совершенно другое дело и это можно рассмотреть. Из нашего опыта следует, что... во многих случаях те, кто... те, кто жалуется на качество тех или иных блок-листов, — это те, кто попал в эти блок-листы и столкнулся с трудностями при удалении себя из этих списков. Как только у нас будут какие-то доказательства того, что тот или иной блок-лист не делает того, о чем заявляет, для нас это будет основанием пересмотреть включение этого списка в наш набор каналов данных, которые мы получаем.

Что касается предоставления данных сообществу, то, как сказано в нашем... в настоящее время мы планируем предоставлять эти данные в общий доступ в рамках инициативы открытых данных. В настоящее время у нас запланировано делать это раз в месяц, но это как решит сообщество. Это мы можем поменять. Скорее всего, мы сможем сделать так, как будет нужно.

ИРАНГА КАХАНГАМА: Спасибо, Дэвид. Кажется, есть еще один вопрос от удаленного участника, который мы пропустили. Я только хочу очень быстро к нему вернуться.

ДЖЕЙМС КОУЛ: Это вопрос от Кристины Розетт (Kristina Rosette) из регистратуры Amazon. «Какие механизмы и процедуры намерена реализовать ICANN, чтобы избежать ложноположительных результатов и потенциальных претензий, прежде чем предоставлять данные DAAR в общий доступ?».

ДЭВИД КОНРАД: Я полагаю, это опять ко мне. Итак, как уже было сказано, мы не сами эти данные формируем. Мы полагаемся на внешних поставщиков, которые предоставляют эти данные по подписке, на основе платных лицензий или свободно. Если

какое-то сообщение считается... так сказать, ложным срабатыванием, то это влияет на то, как эти миллионы пользователей таких репутационных списков блокировки будут взаимодействовать с данным ресурсом, будь то доменное имя или IP-адрес. Ложные срабатывания бывают, это правда. Время от времени мы слышим рассказы о совершенно абсурдных ложноположительных результатах. Однако реальность, в которой мы это рассматриваем... и критерии, по которым мы выбираем тот или иной блок-лист, — это то, что он одобрен отраслевыми и академическими кругами, у него есть документированные процедуры добавления и удаления имен, эти процедуры выполняются, существует понятный механизм работы такого блок-листа.

Знаете, если говорить о вопросах претензий и ответственности, я не юрист и я не буду притворяться юристом по вопросам Интернета.

КЭТРИН БАУЭР-БУЛЬСТ: Большое спасибо, Дэвид. На этом мы переходим к третьей части нашей дискуссии. Итак, в эти последние 12–15 минут мы хотим рассмотреть то, каким образом информирование о нарушениях может поддержать регистратуры и регистраторов в их усилиях по предотвращению нарушений и борьбе с ними. Как это можно использовать в контексте обеспечения выполнения договорных обязательств и в

разработке политик. Мы уже затронули некоторые из этих вопросов. О чем мы еще подробно не говорили, так это о том, как это можно использовать внутри ICANN, и я, пожалуй, подброшу Джейми вопрос о том, учитывали ли вы при разработке этой процедуры ваши потребности и как вы видите возможность использования этой системы отделом соблюдения договорных обязательств в будущем.

ДЖЕЙМИ ХЕДЛУНД: Спасибо. Я никогда не стесняюсь рассказывать о том, что мне нужно. Но мы… мы работали в тесном контакте с офисом технического директора и отдел соблюдения договорных обязательств, на мой взгляд, в целом очень воодушевлен системой DAAR по ряду причин. Одна из них — это то, что она действительно позволяет сосредоточить внимание на данный и фактах при планировании распределения наших ресурсов. Вторая — если правда, что эти списки, из которых состоит платформа DAAR, используются коммерческими предприятиями и другими организациями для принятия решений в отношении служб электронной почты и веб-доступа, такого рода систем, тогда это должно сильно упростить нашу задачу, потому что здесь должна быть встроенная мотивация для тех регистратур или регистраторов, которые могут находиться выше в… в этой иерархии.

Тем не менее нужно внести ясность, знаете, на выходе системы DAAR получаются сводные данные, как объяснил Дэвид. А это не то… мы не можем использовать сводные данные для обеспечения соблюдения договорных обязательств. Нам нужно смотреть на более низкий уровень, чтобы найти фактические доказательства… данные, которые могут служить основанием для действий, которые можно надеяться использовать… для очистки некоторых зон регистратур и регистраторов.

И последнее, что я скажу, это… знаете, те выходные данные, которые я видел, они… демонстрируют, что существует крайне ограниченное, небольшое количество сторон, связанных договорными обязательствами, которые ответственны за подавляющее большинство нарушений, которые можно наблюдать в этих данных. Так что… и часто это даже не те организации, которые… по крайней мере, я не видел, чтобы они когда-либо как-то активно участвовали в работе ICANN. Так что я считаю, что если мы можем… если мы сможем использовать эти данные и добиться какого-то прогресса, то это будет не только, так сказать, хорошо для пользователей и Интернета вообще, я думаю, это будет также хорошо для поддержки доверия и легитимности ICANN и модели работы с участием многих заинтересованных сторон, а это, как вы знаете, после передачи координирующей роли в

исполнении функций IANA является важным вопросом, находящимся в центре нашего внимания.

ИРАНГА КАХАНГАМА: Спасибо, Джейми. О, Алан. Прошу вас.

АЛАН ВУДС: Я хочу только очень быстро поблагодарить Джейми за эти слова. Приятно это слышать. Я также хотел подчеркнуть, что да, действительно, существуют злоумышленники и, знаете, существует огромное количество регистратур, которые действительно делают все от них зависящее, чтобы решать эти задачи, подключаться, выполнять какие-то упреждающие действия, участвовать в конференциях ICANN и проводить такие дискуссии. Я хочу сказать, с моей точки зрения, с точки зрения Donuts, мы однозначно поддерживаем обеспечение соблюдения требований. Если у нас будут доказательства, если это будет сделано и даст нам возможность принимать решения, если можно будет протестировать эти доказательства таким образом, тогда совершенно точно да. Я хочу сказать, что мы были бы очень рады этому.

ИРАНГА КАХАНГАМА: Спасибо. Грэм, вы поднимали руку? Нет.

ГРЭМ БАНТОН: Извините. Как бы нет. Для протокола: это Грэм. Знаете, регистраторы очень поддерживают идею устранить злоумышленников с платформы. Это облегчило бы нагрузку на остальных из нас, на тех, кто очень много работает над недопущением нарушений на наших платформах. И это также позволило бы устранить множество осложнений с точки зрения политик, поскольку мы стремимся находить решения путем выработки политик, которые действовали бы для всех сторон, связанных договорными обязательствами или для всех регистраторов, хотя на самом деле эти решения должны быть узкими и нацеленными на конкретных злоумышленников. Так что если мы к этому придем, то, на мой взгляд, это позволит решить множество проблем и облегчит жизнь для всех нас. Спасибо.

ИРАНГА КАХАНГАМА: Микрофон номер один.

ГРЕГ МУНЬЕ (GREG MOUNIER): Здравствуйте. Грег Мунье из Европола. У меня вопрос к Грэму и Алану. Отрасль доменных имен руководствуется интересами получения прибыли, и мне кажется, что такие проактивные меры по предотвращению нарушений зачастую расцениваются в отрасли как дополнительные затраты. Поэтому у меня такой вопрос: как можно… что нужно для того, чтобы как-то обратить эту логику вспять, чтобы отрасль

воспринимала такие проактивные меры по предотвращению нарушений как конкурентное преимущество. То есть, иными словами, когда мы увидим, к примеру, в рекламной стратегии Tucows заявление о том, что Tucows обеспечивает самый низкий уровень нарушений, значит, с нами вы в безопасности, значит, вы сможете больше заработать.

[Аплодисменты]

ГРЭМ БАНТОН: Спасибо, Грег. Для протокола: это Грэм. Это хороший вопрос. Не знаю. Я думаю, что проактивный подход также подразумевает определенную ответственность, что также нужно учитывать, анализируя показатели прибыльности. То есть технологии нужно прийти к какому-то этапу, на котором мы смогли бы предпринимать такие упреждающие меры в отношении регистрации каким-то таким образом, который, на мой взгляд, пока невозможен или, по крайней мере, я лично такого не видел.

ИРАНГА КАХАНГАМА: Род, вы хотите дополнить?

АЛАН ВУДС: Это Алан Вудс, я тоже здесь. Donuts тоже. Я хочу сказать, мы очень серьезно к этому относимся. И я хочу сказать, что это неотъемлемая часть нашего нынешнего подхода к

злоупотреблениям DNS. Однако я хочу сказать, что мы входим в такие организации, как Ассоциация доменных имен и Инициатива безопасных доменов, мы пытаемся участвовать в таких отраслевых инициативах, в каких-то добровольных начинаниях, что выделяет нас и отличает нас от злоумышленников. И мы, опять же, делаем это.

Кроме того, знаете, каждый раз, когда мы останавливаем работу какого-то домена, это, по сути, урок для злоумышленника, из которого он делает вывод, что нужно уйти куда-то еще. И это еще одна проблема, о которой нам нужно задуматься. Мы можем вытеснить их с нашей платформы, однако они просто найдут для себя другую платформу, более удобную для злоумышленников. То есть нам нужно сосредоточить внимание также на том, что избавиться от таких недобросовестных платформ.

ИРАНГА КАХАНГАМА: Спасибо. Я хочу… (называет имя) в очереди, так что я хочу дать ему возможность высказаться.

РОД РАСМУССЕН: Спасибо. Это снова Род Расмуссен. Итак, это… этот самый первый пункт нашего обсуждения — это та причина, по которой я приехал на мою первую конференцию ICANN. Я представлял отрасль борьбы с нарушениями и пытался наладить дискуссию с регистраторами. К сожалению, это

была конференция в Ванкувере, на ней произошло много чего другого, что не позволило этой дискуссии набрать должный вес. Вы можете ознакомиться с историей сами. Как бы то ни было, я хочу сказать… и это было больше десяти лет назад. И многое из этого было сделано и было сделано успешно. Есть множество примеров. Один из таких примеров — это то, что антифишинговая рабочая группа, я и Грег Аарон (Greg Aaron), которого многие из вас знают, мы готовим периодический отчет, мы делаем это начиная с 2007 года, посвященный тенденциям регистрации доменных имен, которые используются для фишинга. Эти отчеты используются вместе регистраторами и регистратурами для определения проблем и тенденций и формирования политик в отношении таких проблем. И это касается как пространства ICANN, так и пространства ccTLD. В частности, национальные домены верхнего уровня, ccTLD, сталкивались с большими проблемами и смогли решить их благодаря анализу тенденций и шаблонов.

Более того, многие регистраторы и регистратуры организовали различные механизмы отчетности, автоматизированные механизмы отчетности, на основе различных технологических платформ. В качестве одной из таких платформ используются договорные отношения. В моей прошлой жизни у меня была компания, которая заключала договора с такого рода организациями и выступала в роли их

представителя в выяснении того, являлись ли те или иные действия нарушениями и могли ли они служить основанием для прекращения работы. Еще можно назвать программу доверительного посредника, когда вы проходите специальную аккредитацию и затем можете передавать роль в таких доверительных отношениях кому-то еще, обладающему необходимой для этого квалификацией. Так что я повторюсь, это все можно автоматизировать и делегировать, такие модели действительно существуют. Вопрос больше в том, чтобы сделать эту информацию общедоступной, чтобы люди могли пользоваться такими моделями. Спасибо.

КЭТРИН БАУЭР-БУЛЬСТ: Вы идеально уложились во время, Род. Итак, у нас микрофон номер один.

ДЭВИД ТЭЙЛОР: Спасибо. Я Дэвид Тэйлор из компании Hogan Lovells. Я юрист, так что можете сейчас меня освистать, но я также член группы по анализу конкуренции, потребительского доверия и потребительского выбора, так что можете меня поддержать. То есть я вон с тем бородатым чудаком. На самом у меня вопрос, который касается информирования о нарушениях, это, разумеется, ключевая проблема, и есть множество хороших регистраторов и множество плохих регистраторов.

Есть множество хороших регистраторов и немного плохих регистраторов. И мы знаем, когда мы занимаемся конкретными проблемами, что иногда может потребоваться довольно много времени, чтобы тот или иной отдельный регистратор остановил работу доменного имени, даже если налицо очевидные факты нарушений и незаконной деятельности. Я имею в виду совершенно очевидные факты. Которые запросто были бы подтверждены в суде. И все равно может понадобиться три-четыре недели работы, чтобы они остановили работу этого домена. То есть мы могли бы обратиться в отдел соблюдения договорных обязательств ICANN, и в некоторых случаях мы так и делаем.

Однако когда вы берете регистратора, который, как показал перед этим Дрю, если взять того, которого закрыли… и, Джейми, мы об этом говорили, однако вы упомянули регистратора AlpNames… когда там такой высокий уровень нарушений, например, когда в домене .SCIENCE 51% файла зоны — это доменные имена, используемые для злоупотреблений, и вы видите, что они все еще работают и не закрыты, и вы видите, что регистратор все еще не аккредитован, хотя прошел уже год или, может, полгода. Для непосвященных, как… почему в таких случаях требуется так много времени, хотя ситуация настолько очевидна и однозначна? Разумеется, есть какие-то причины, и если вы не можете о чем-то говорить, то и не говорите, но я просто

пытаюсь… я не могу это понять и я не могу это объяснить моим клиентам.

ДЖЕЙМИ ХЕДЛУНД: Итак, в общем случае тут есть два момента. Один — это то, что зафиксированные свидетельства и сводные данные, свидетельствующие о том, что какая-то из сторон, связанных договорными обязательствами… отличается высоким уровнем злоупотреблений, этого недостаточно. Нужны фактические доказательства, чтобы мы могли… перейти дальше.

А второе — это определенные ограничения, которые есть в самих договорах. То есть мы не можем по собственной инициативе распорядиться приостановить работу домена, к примеру, или закрыть этот домен.

И один момент, который, я считаю… который, я надеюсь, мы получим благодаря использованию данных платформы DAAR и лежащих в ее основе… некоторых имен, это то, что мы сможем видеть, где мы работаем успешно, а где нет. То есть там, где нам не удается добиться успеха и где злоумышленники не прекращают свою деятельность, несмотря на наши… наши усилия по использованию тех инструментов, которые есть в нашем распоряжении, тогда эта информация будет поступать в сообщество и сообщество сможет использовать ее при разработке политик.

То есть даже в тех случаях, когда у нас не получится помочь очистить пространство регистраторов и регистратур, сообщество и все мы будем иметь, так сказать, информацию о том, что где не сработало, так что хочется надеяться, что это станет источником... стимулом для изменения политик или договоров.

ИРАНГА КАХАНГАМА: Спасибо, Джейми. Очень быстро. Последний комментарий, прежде чем мы будем закругляться. Я хочу дать возможность высказаться Дениз как еще одной из затрагиваемых сторон во всей этой теме отчетности и как это будет использоваться в выработке решений.

ДЕНИЗ МИШЕЛЬ: Разумеется. Итак... в отчете SADAG, в отчете группы CCT о злоупотреблениях было показано, что новые gTLD сталкивались с уровнем злоупотреблений, который почти в десять раз превышал уровень злоупотреблений для старых gTLD. Данные о злоупотреблениях, которые были представлены в этом отчете, и связанная с ними информация были очень полезны и важны, к примеру, для процесса разработки политики в отношении механизма защиты прав, который проходит в настоящее время, а также для процесса разработки политики в отношении последующих процедур, который также проходит сейчас и который позволит создать...

который посвящен созданию политик для следующего раунда ввода новых gTLD.

Это всего лишь один пример. Есть много других, которые касаются таких вещей, как реализация служб защиты конфиденциальности и регистрации через доверенных лиц и других инициатив, осуществляемых в рамках ICANN.

Однако на самом деле все сводится к тому, чтобы иметь данные о злоупотреблениях, а также информацию о тенденциях, которую можно использовать как основу для множества различных действий в рамках ICANN. Мы должны быть сообществом, использующим реальные факты и данные для обеспечения понимания, в качестве фундамента при принятии решений. Это очень и очень важно. Так что, Дэвид, если мы можем что-то сделать, чтобы помочь юристам, чтобы переместить отчет DAAR в публичную сферу, мы можем воспользоваться инициативой открытых данных, там, кажется, опять началась работа, потому что до этого данные не менялись четыре месяца, то это было бы очень полезно. И мы действительно надеемся, что сможем поддержать эти усилия в будущем.

Спасибо.

ДЭВИД КОНРАД: Просто в качестве пояснения. Я, конечно, пошутил, когда сказал, что юристы блокируют деятельность в этом

направлении. Нам приходится продвигаться путем переработки лицензионных соглашений, а это занимает определенное время. Мы практически уверены в том, что сможем продвинуться (неразборчиво) статистических отчетов в самом ближайшем будущем, а более обширная и всеобъемлющая информация в формате электронных таблиц, вы можете себе это представить, она должна быть готова вскоре после этого.

КЭТРИН БАУЭР-БУЛЬСТ: Хорошо. Спасибо, Дэвид. У нас заканчивается время, поэтому мы не сможем больше принимать вопросы. Прошу прощения. Я думаю, что эти дебаты продемонстрировали, что нам нужно проводить больше дебатов. Мы собрали в одном месте разные точки зрения на проблему противодействия злоупотреблениям и я считаю, что это получилось очень неплохо в том, что касается озвучивания различных потребностей разных частей сообщества, от разработки политик до отдельных действий, будь то упреждающие действия или реагирование, и это помогло нам определить способы возможного использования данных и информирования проекта DAAR.

И я считаю, что в обмене мнениями между Дэвидом и Джейми был поднят один очень важный момент, а именно то, что существует очень небольшое количество сторон, связанных

договорными обязательствами, в которых концентрирована большая часть злоупотреблений, и именно в этом, с нашей точки зрения, сводные данные и конкретная информация сходятся, потому что, конечно же, есть какие-то меры, которые могут предприниматься. Даже если в тех 76 примерах, которые привел Дрю, будет два ложноположительных результата, все равно у нас будет достаточно других данных для принятия каких-то мер.

Возможно, в будущем нам понадобится проанализировать, как можно уменьшить этот разрыв между сводными данными и конкретными доказательствами, на основании которых можно предпринимать какие-то действия. А для этого... я думаю, мы можем еще вернуться к этой идее о принципах, о которой говорил Иранга в своем вступительном слове, и на этом я передаю ему слово, чтобы он мог продолжить.

ИРАНГА КАХАНГАМА: Спасибо.

Я хочу поблагодарить всех за участие в этой дискуссии. Я думаю... да, я думаю, важно двигаться дальше в этой дискуссии, так что, думаю, я заранее попрошу рабочую группу по обеспечению общественной безопасности как бы помочь нам в направлении нашего диалога. Однако я считаю, что наше сообщество заслуживает возможность использовать надлежащий механизм, который позволял бы организовать и

объединить все эти вопросы на уровне сквозной работы сообщества для продвижения в решении проблем. Так что я считаю, что мы еще вернемся и попытаемся подумать о том, как наилучшим образом продвинуться в решении некоторых из этих проблем и как предоставить в распоряжение сообщества нужные механизмы для дальнейшей работы в рамках усилий по борьбе со злоупотреблениями DNS. И я надеюсь, что мы сможем воспользоваться этим как неким форумом, который позволит нам поддерживать работу сообщества на должном уровне, а также обеспечивать прозрачность и открытость этого сообщества для продвижения в решении проблем на этом фронте.

Так что я хочу поблагодарить всех, кто присоединился к нам в этот раз и, я надеюсь, будет участвовать и в будущих подобных заседаниях.

Спасибо.

[Аплодисменты]

[КОНЕЦ СТЕНОГРАММЫ]