ICANN76 | ФОРУМ СООБЩЕСТВА - Обсуждение GAC: Злоупотребление DNS
Вторник, 14 марта 2023 года - 10:30 - 12:00 КАНКУН

JULIA CHARVOLEN: Здравствуйте и приветствуем вас на дискуссии GAC на ICANN76 о злоупотреблениях DNS во вторник, 14 марта, в 10:30 по местному времени. Пожалуйста, обратите внимание, что это заседание записывается и регулируется Ожидаемыми стандартами поведения ICANN.

Во время этого заседания вопросы или комментарии, представленные в чате, будут зачитаны вслух, если они будут изложены в надлежащей форме. Если вы хотите выступить, пожалуйста, поднимите руку через Zoom. Не забудьте назвать свое имя и язык, на котором вы будете говорить, в случае, если вы будете говорить не на английском языке. Говорите четко и в разумном темпе, чтобы обеспечить точный перевод. Пожалуйста, не забудьте отключить звук всех других устройств во время выступления. Вы можете воспользоваться всеми доступными функциями для данного заседания на панели инструментов Zoom.

И с этим я передаю слово нашему председателю GAC. Манал Исмаил (Manal Ismail), пожалуйста.

MANAL ISMAIL: Большое спасибо, Джулия. Всем доброго утра, доброго дня и доброго вечера. С возвращением. Это обсуждение GAC по борьбе со злоупотреблениями DNS, запланированное на час. В ходе этого

заседания мы продолжим рассмотрение GAC инициатив корпорации ICANN и сообщества ICANN по предотвращению и борьбе со злоупотреблениями DNS.

Кроме того, мы будем проинформированы о соответствующих событиях и продолжим обсуждение возможных усилий GAC по взаимодействию с более широким сообществом ICANN для поддержки усовершенствованных пересмотров договоров и возможных процессов разработки политики для более эффективной борьбы со злоупотреблениями DNS.

Итак, без лишних слов позвольте мне передать слово нашим ведущим по теме. С нами Габриэль Эндрюс (Gabriel Andrews), Федеральное бюро расследований США; Лорин Капин (Laureen Kapin), Федеральная торговая комиссия США и сопредседатель PSWG GAC; и Крис Льюис-Эванс (Chris Lewis-Evans), Национальное агентство по борьбе с преступностью Великобритании и сопредседатель PSWG GAC. Передаем слово вам, Крис, пожалуйста.

CHRIS LEWIS-EVANS: Большое спасибо, Манал. Доброе утро, добрый день и добрый вечер всем. Переходим к следующему слайду, пожалуйста. Мы собираемся провести заседание по злоупотреблению DNS, и у нас есть внешняя презентация. Я вижу в углу руководителя сети по вопросам интернета и политики юрисдикции, который, надеюсь, разбирается с некоторыми слайдами вместе с персоналом поддержки GAC.

Так что сначала я сделаю небольшое вступление и расскажу о том, почему борьба со злоупотреблениями DNS важна. Затем мы сделаем

презентацию о статистике киберпреступлений и о том, как она связана со злоупотреблениями DNS. Затем мы рассмотрим другие мероприятия, проводимые в рамках сообщества. А затем подведем итоги и обсудим либо рекомендации для коммюнике, либо важные для нас вопросы. Перейдите, пожалуйста, к следующему слайду. Спасибо.

Я практически чувствую, что мне не нужно делать этот слайд. Похоже, мы довольно часто говорим о злоупотреблении DNS. На этой конференции уже было несколько действительно хороших заседаний. Я еще раз прокомментирую семинар по наращиванию потенциала в субботу. Там была проведена хорошая сессия по злоупотреблению DNS, о которой вы можете прочитать в этом разделе.

Здесь у нас есть несколько ссылок, по которым вы можете перейти. Как всегда, вы можете выполнить поиск на сайте GAC по теме злоупотребления DNS, и это приведет к появлению пунктов коммюнике, по которым работает персонал поддержки. Бенедетта и другие сотрудники поддержки действительно поддерживают эту информацию в актуальном состоянии. Они делают очень хорошую работу, предоставляя ресурсы, которые мы можем там искать. Итак, у нас есть ряд пунктов, которые мы отмечаем.

Это очень важная часть работы PSWG. Это входит в наш план работы, который мы ратифицировали и одобрили на данной конференции, что было действительно хорошо, для нас, чтобы поддержать потребности правоохранительных органов и сотрудников общественной безопасности в защите населения, что они действительно делают в этом направлении.

Как я уже сказал, в обществе многое происходит, поэтому это важно для других заинтересованных сторон в обществе. Идет много обсуждений, консультаций с Правлением и переписки. Бизнес-сообщество прислало немало материалов о том, как это важно для них. Были также группы по анализу - группа по анализу CCT, RDS-WHOIS2, SSR2 и другие, а также PDP от GNSO по последующим процедурам, которые касаются злоупотребления DNS.

Другая, которую мы затронем позже в презентации, - это усилия от палаты сторон, связанных договорными обязательствами. Они направили в Правление письмо с просьбой открыть переговоры по договору, чтобы помочь решить проблему злоупотребления DNS. Это действительно хороший шаг. Он просто показывает, что все в сообществе хотят принять меры, и это действительно важно для всех, именно поэтому мы рассматривали этот вопрос в течение некоторого времени.

Затем - и я просто хочу быстро обратиться к нашему персоналу поддержки - мы близко?

LAUREEN KAPIN: Нет.

CHRIS LEWIS-EVANS: Нет. Хорошо. Так что, Гейб, может быть, стоит предупредить.

LAUREEN KAPIN: Именно здесь мы можем проявить гибкость и показать, что мы адаптируемся к текущим обстоятельствам, и что мы способны переключаться с одного направления на другое.

CHRIS LEWIS-EVANS: Да. Смотрите, Гейб. Вы следующий. Итак, мы переходим к нашей презентации о тенденциях киберпреступности. Итак, можем ли мы перейти к двум слайдам, я думаю, в пакете? Спасибо. Гейб, вам слово. Спасибо.

GABRIEL ANDREWS: Спасибо. Здравствуйте. Меня зовут Габриэль, я выступаю здесь в качестве члена Рабочей группы по вопросам общественной безопасности. То, что мы надеемся сделать здесь, - это то, что мы, возможно, оптимистично настроены, что мы сможем делать это на ежегодной основе позже. Но причина этого в том, что когда речь идет о понимании масштабов злоупотребления DNS, точно так же, как и при попытке понять масштабы интернет-преступности, важно признать, что у нас нет точных фактов. Зато у нас есть множество различных точек зрения.

Так что, подобно слепому на этой картинке, которую вы можете узнать с семинара по наращиванию потенциала - я тоже использовал ее там - у нас есть множество людей, которые делают все возможное, чтобы наблюдать за тем, что находится перед ними, говорить о том, что они воспринимают, в надежде, что, сотрудничая, мы сможем получить лучшее представление о том, что на самом деле происходит.

И вот здесь я понимаю, что существует множество замечательных усилий сообщества, направленных на предоставление данных, метрик, измерений, наблюдений за злоупотреблениями DNS. Я думаю о таких вещах, как отчетность Compass Института злоупотреблений DNS, которая начала действовать осенью прошлого года. Например, OCTO ICANN и их отчетность о злоупотреблениях доменами.

Я слышал, что буквально два дня назад в разговоре с исполнительным персоналом Джон Крэйн (John Crain) упомянул, что в дополнение к тому, что мы уже ожидаем от отчетности о злоупотреблениях на уровне регистраторов, у него есть идеи о предиктивной аналитике и машинном обучении, которые он хочет включить. Мне очень интересно посмотреть, что получится из этих усилий.

Но в дополнение к этим усилиям, предпринимаемым сообществом, мы надеемся предоставить дополнительные перспективы, которые могут привнести только правоохранительные органы и которые исходят только от общественной безопасности. Я имею в виду обращения жертв, которые поступают к нам.

Для ясности, мы не утверждаем, что все интернет-преступления - это злоупотребления DNS. Скорее, мы понимаем, что объем и масштаб ущерба, причиненного жертвам, о котором нам сообщают, может быть, одной из тех перспектив, которые, по вашему мнению, важно учитывать при обсуждении, особенно если мы можем быть полезны в каком-то небольшом смысле, помогая перевести эти сообщения на то, как и где они связаны со злоупотреблением DNS. И на этом, я думаю, Крис, у вас есть первая часть этого.

CHRIS LEWIS-EVANS: Да. Только очень коротко, перед тем как мы перейдем к следующему слайду. Извините. Мы можем вернуться на один слайд назад? Спасибо. На нашем последнем заседании PSWG мы обратились ко всем членам с просьбой предоставить нам статистические данные о киберпреступности и о том, как она может быть связана со злоупотреблением DNS.

На данный момент мы не получили никаких других сообщений, кроме США и Великобритании. Так что если вы работаете с вашими правоохранительными органами или агентствами по защите прав потребителей, то, пожалуйста, не стесняйтесь направить их в нашу сторону. Нам было бы очень интересно узнать, что видят другие страны, и сделать этот обзор статистики более широким. И мы планируем делать это, вероятно, раз в год, чтобы дать вам представление о ситуации.

Если перейти к слайдам по Великобритании, то в Соединенном Королевстве у нас есть единый орган отчетности под названием Action Fraud, который занимается не только мошенничеством. Они также занимаются киберпреступностью. Но сначала было название, а потом они добавили к нему еще и этот мандат.

Их четыре основных статистических показателя по сбору данных на самом деле не отслеживают злоупотребления DNS. У них есть хакерство, социальные сети и электронная почта. Вирусы и вредоносные программы, то есть, вроде как, вредоносные программы, но вирусы тоже присутствуют, поэтому они не совсем соответствуют тому, что мы понимаем под злоупотреблением DNS. И

затем хакерство, будь то личное или вымогательство, которое, как правило, больше ориентировано на программы-вымогатели. Итак, как вы можете видеть на этом слайде, данные за 2014 год и общая тенденция к увеличению количества сообщений о таких преступлениях. Перейдите, пожалуйста, к следующему слайду.

Кроме того, они проводят опросы среди предприятий и благотворительных организаций, чтобы получить представление о том, как они пострадали, что они видят и как справляются с ситуацией. Этот фрагмент анализа касается того, сколько организаций выявили нарушения или атаки на свои системы. Итак, все довольно статично, может быть, небольшая тенденция к снижению на стороне бизнеса. Но очень интересно, что в благотворительных организациях наблюдается определенный рост.

Некоторые из мыслей, стоящих за этим, заключаются в том, что благотворительные организации до GDPR, возможно, не были настроены на то, чтобы изучать свои собственные сети и проводить анализ. Как только вы начинаете что-то искать, вы, как правило, это находите. Так что является ли это одной из причин такого роста - то, что они искали это и нашли, или это рост целевых атак, - сказать очень сложно. Это может быть и то, и другое, так что сказать довольно сложно. Но это лишь небольшая тенденция. И перейдем к следующему слайду, пожалуйста.

На этом слайде, очевидно, тех, кто пострадал от атаки, спрашивали о том, как они идентифицировали эту атаку и каков был первоначальный вектор атаки. На протяжении многих лет ответом на этот вопрос в 80 примерно процентах случаев был фишинг. Фишинг определенно относится к злоупотреблениям DNS. Таким образом, вы

можете видеть, что из всех других преступлений, которые я привел в первой подборке, 80% или около того связаны с фишингом, или начальным вектором атаки был фишинг. Таким образом, сократив количество фишинга, мы можем оказать реальное влияние на ущерб, наносимый другими преступлениями, с которыми мы имеем дело на ежедневной основе.

Второе сверху немного похоже на фишинг. Но здесь больше внимания уделяется похожим доменам, поддельным письмам и тому подобным вещам. На них приходится чуть меньше остальной части. Очевидно, что некоторые из них могут немного пересекаться. Следующий слайд, пожалуйста.

Тот же вопрос к благотворительным организациям и очень похожий ответ. Опять же, 80% - фишинг. Таким образом, если мы сможем помочь в борьбе со злоупотреблениями DNS и фишингом, это окажет значительное влияние на снижение количества преступлений, от которых страдают эти компании и благотворительные организации. Следующий слайд, пожалуйста

В Великобритании есть служба, которая называется Служба сообщений о подозрительной электронной почте (Suspicious Email Reporting Service). Не только ICANN любит аббревиатуры. Она была создана в 2020 году, и это служба, в рамках которой частные лица или компании могут сообщать правительству о подозрительных электронных сообщениях. Там есть подробности. Они принимают пересылки по электронной почте, а также SMS-сообщения, поскольку это еще один крупный источник фишинговых сообщений. В течение 2022 года мы получили 6,4 миллиона сообщений в эту

службу. Так что это очень масштабно. Множество жертв в Великобритании и людей, сообщающих об этом.

Как я уже сказал, служба была запущена только в 2020 году, очевидно, в качестве ответной меры на некоторые действия, которые предпринимались во время пандемии. Но с момента запуска в эту службу поступило 15,8 миллиона сообщений. И это тенденция к росту, но на данный момент нет достаточного количества данных, чтобы показать это. Так что в ближайшие годы я, несомненно, помещу это на небольшой красивый график.

Затем, в связи с этим, правительство может увидеть из этой отчетности, что они пытаются выдать себя за правительственную организацию. Так, в рамках этих фишинговых атак они представляли нашу службу здравоохранения, наше лицензирование телевидения, наши налоговые и таможенные органы, а также сайт gov.uk. Это сайт, на котором мы размещаем всю нашу общественную информацию, будь то советы о том, что делать с COVID, советы по путешествиям. Там есть все. И еще один - это агентство по лицензированию водителей и транспортных средств. Таким образом, определенно много правительственных атак, и эта служба помогла устранить некоторые из них. Следующий слайд, пожалуйста.

Я коснулся бизнеса. Теперь очевидно, что частные лица и пользователи Интернета также подвергаются этому воздействию и сообщают нам о преступлениях. Был проведен телефонный опрос ряда жертв, обратившихся к нам, чтобы понять, как это повлияло на них с финансовой точки зрения.

Вы можете посмотреть здесь. Это ужасный график. Извините. Это то, что мне дали. Но вы можете видеть здесь диапазон от 20 до 250 фунтов - это, вероятно, большая часть того, что люди потеряли. Но если подумать, это не так много денег. Но потом, у нас было 6,4 миллиона, в этом году, людей, которые заявили о преступлении. И если вы скажете, что каждый из них потерял хотя бы 20 фунтов, то 20 раз по 6,4 миллиона - это неплохая дневная или годовая работа.

Так что, когда вы смотрите на это, все очень масштабно. Это может показаться незначительным. Однако, очевидно, особенно в настоящее время, с кризисом стоимости жизни, который мы имеем в ряде стран, для людей потеря этих денег действительно имеет большое значение. Следующий слайд, пожалуйста.

Мы много говорим о деньгах в сфере киберпреступности. И это не только деньги, которые влияют на людей, особенно на частных лиц. Предприятия страдают от потери данных, и это сказывается на них. Но и на индивидуальном уровне это может быть очень важно и может очень расстроить их.

Я просто расскажу об этом на конкретном примере. В нашу полицейскую систему поступила информация о 17-летнем подростке, который сообщил, что хакер запрашивает больше паролей и имеет доступ к ряду его аккаунтов в социальных сетях.

Мы смогли проделать определенную работу на основе этой информации. Нам удалось установить личность подозреваемого, выяснить, что у него была история взлома аккаунтов в социальных сетях ряда лиц. В результате мы получили ордер на посещение его домашнего адреса и обнаружили несколько активных телефонов,

которые он использовал для совершения некоторых из этих преступлений. На этих телефонах были обнаружены следы массового фишинга. Перейдите, пожалуйста, к следующему слайду.

Это пример одного из сообщений. Здесь вы увидите, что он представляется человеком, который нашел некоторую информацию о человеке и говорит: "Я нашел несколько ваших изображений на сайте. Возможно, вы захотите что-нибудь с этим сделать". Человек отвечает и спрашивает: "Какая ссылка?". И тогда этот человек публикует ссылку, по которой они могут перейти.

Изучив телефоны, мы обнаружили сотни сообщений, отправленных молодым девушкам, как правило, с попыткой получить доступ к их аккаунтам. Таким образом, вы видите, что с одного домена или одного человека у него могут быть сотни жертв. Это не аналог: один домен - одна жертва. Это может быть один домен, сотни жертв. Все зависит от типа атаки и способа ее использования, как это работает. Мы также изучили этот сайт, чтобы понять, как этот человек использовал его для вымогательства у других людей. Перейдите, пожалуйста, к следующему слайду.

Этот слайд будет немного загруженным, поэтому я заранее прошу прощения, и немного маленьким, но он маленький не просто так. В правом верхнем углу экрана находится фишинговая служба, размещенная в Интернете, которая дает зарегистрированным пользователям возможность покупать фишинговые страницы и иметь их в Интернете. Итак, вы нажимаете на одну из них, будь то Netflix, Facebook, Snapchat или любая другая. Вы даже можете выбрать язык, на котором хотите ее видеть. Здесь очень мелко, но есть английский, испанский, французский и русский, кажется, все.

Так что вы можете выбрать языки, на которых хотите появляться. Вы платите за эту услугу.

И затем, внизу слева, есть пример Snapchat. Он создает вредоносный домен, который вы можете прикрепить к своему сообщению. После этого он будет собирать для вас информацию. На нижнем рисунке - пример информационной панели, которую они создают, чтобы вы могли просмотреть все свои собранные учетные данные.

Очевидно, что как только они собирают эти учетные данные, они начинают заниматься вымогательством. Они забирают изображения, которые хранятся там, независимо от того, являются ли они частными, если это был Google Drive, если они даже не были опубликованы в социальных сетях. Так что это действительно сильно влияет на людей.

Мы смогли убрать этот сайт при поддержке регистраторов. Так что спасибо вам за это. В следующем месяце этот человек предстанет перед судом, но в настоящее время он находится под стражей из-за угрозы, которую он представляет для числа жертв. Это очень важно.

Мы, разумеется, попытались связаться с каждой жертвой, которую нам удалось идентифицировать, и сообщить им, что мы защитили их данные, удалили их, и предложить им обновить свои пароли и все остальное. Очень важно понять, как это повлияет на них. У нас было так много обращений: "О, спасибо, что вы это сделали. Я не знал, как это решить". И здесь очень важно, как мы можем решить эту проблему и как мы можем устранить часть причиняемого вреда.

Затем переходим к следующему слайду. Думаю, я передаю слово Гейбу.

LAUREEN KAPIN: Мне интересно, как обстоят дела с презентацией нашего коллеги, Бертрана. Готовы ли вы начать? Вы бы предпочли начать сейчас или вы бы предпочли... Что вы думаете?

CHRIS LEWIS-EVANS: Я думаю, мы сделаем ту, что у Гейба, потому что она очень хорошо продолжает тему. Потом мы остановимся. Извините. У меня есть еще один слайд. Это просто подведение итогов по данным о бизнесе и по отдельным людям. Последний отчет был за 2020-2021 годы. В Великобритании они получили 875 000 сообщений о мошенничестве и киберпреступлениях. Извините. Это должно быть оба вместе. В этом отчете говорится о потерях на сумму 2,35 миллиарда.

При этом 80% этих мошенничеств были совершены с помощью кибернетических средств, будь то фишинговое электронное письмо или что-то другое. Таким образом, большая часть этих потерь связана с той или иной формой кибер-активности. И, как мы уже говорили, фишинговые сообщения электронной почты - 80% от этого числа, так что для преступников это действительно важный фактор, который они используют для инициирования своих кибератак. И это, безусловно, последний слайд перед тем, как я передам слово Гейбу.

GABRIEL ANDREWS: Можем ли мы посмотреть следующий слайд? Спасибо. С точки зрения США. И опять же, как сказал Крис, мы очень надеемся, что есть и другие люди, которые могут побудить свои

правоохранительные органы поделиться перспективами со всего мира.

ФБР только что опубликовало на прошлой неделе свой отчет об интернет-преступлениях за 2022 календарный год, так что это самая свежая информация. Именно поэтому я считаю, что возможность говорить об этом на ежегодной основе - это хорошо, потому что нам нравится иметь возможность делиться этой информацией, когда она выходит и пока она свежая.

Эти данные представляют собой сводку всех жалоб жертв, которые поступают в наш Центр жалоб на преступления в Интернете. Это централизованный портал, с помощью которого мы получаем и обобщаем все эти данные. Затем они обрабатываются и публикуют отчеты, основанные на этих данных. Но следует отметить, что это не картина всех существующих интернет-преступлений. Это только то, о чем нам сообщают. Следующий слайд, пожалуйста.

За последние пять лет IC3 - опять же, это сокращение названия Центра жалоб на преступления в Интернете - получал в среднем около 650 000 жалоб в год. В среднем это составляет чуть более 2000 жалоб в день, так что это довольно большое число. Но оно все еще сильно недооценивает истинное количество преступлений. Мы знаем, что не всегда получаем все жалобы.

Интересно отметить, что если посмотреть на количество фактических жалоб - это те люди, которые обращаются к нам - оно оставалось относительно стабильным в течение последних трех лет, что интересно. Но объем потерь неуклонно растет. Хотелось бы иметь

хорошее объяснение, почему это так. На данный момент у нас нет толкового объяснения, но это, безусловно, интересно отметить. Это показывает, что вред продолжается, даже если относительное количество жалоб остается стабильным. Пожалуйста, перейдите к следующему слайду.

Как упомянул Крис в своих категориях преступлений и как они их объединяют, мы также не отслеживаем злоупотребления DNS как категорию. Но есть категории злоупотреблений DNS, которые отслеживаются в наших отчетах IC3. И я, в частности, отмечаю здесь, в самом низу, фишинг. Когда мы смотрим на пять основных категорий интернет-преступлений, о которых нам сообщают, мы видим, что фишинг является основной категорией.

Более того, поскольку здесь показаны данные за последние пять лет, вы можете увидеть, что по тем или иным причинам фишинг сильно вырос по сравнению с пятью годами назад и достиг сегодняшнего уровня, по крайней мере, с точки зрения жалоб, которые мы получаем. Следующий.

Здесь снова показаны все категории преступлений, а не только пять основных, и показано, как фишинг связан с ними. Как уже отметил Крис, следует подчеркнуть, что фишинг, хотя он и отслеживается как отдельная категория, часто является первоначальным методом, который злоумышленники используют для нанесения ущерба жертвам ряда других категорий преступлений, которые также существуют в этом разделе.

В качестве примера вы можете спросить: "Является ли программа-вымогатель злоупотреблением DNS?". Нет. Это не так. Программа-

вымогатель - это когда злоумышленник забирает ваши данные на вашем устройстве, шифрует их и не дает вам их получить, пока вы не заплатите выкуп. Но если вы зададите вопрос: "Распространяется ли программа-вымогатель с помощью фишинга?", то ответ будет положительным.

На прошлой неделе вышел отчет о новом варианте программы-вымогателя под названием Royal ransomware от CISA, одного из моих родственных агентств. В этом отчете они подсчитали, что 67% заражений программой-вымогателем Royal ransomware произошло в результате фишинга. Опять же, мы отслеживаем начальную категорию, но она имеет влияние и на другие категории.

Таким образом, если говорить более развернуто, когда наши друзья, сотрудники и коллеги в сообществе ICANN, существующие на уровне регистраторов или регистратур, предпринимают ответственные действия по борьбе со злоупотреблениями для решения проблемы злонамеренно зарегистрированных доменов, которые используются для фишинга, они помогают бороться не только с наиболее часто регистрируемым видом интернет-преступлений, но и со всеми другими категориями, которые становятся возможными благодаря этому. Следующий слайд.

Помимо того, что я поделился статистикой из ежегодного отчета, я также спросил у своих коллег: "Эй, что новенького? Что нового, предстоящего и определяющего тенденции? Что примечательного произошло за последние месяцы?". И вот что они мне ответили - это то, что они называют "malvertising". Для удобства переводчиков это сочетание слов "вредоносное ПО" (malware) и "реклама" (advertising). Это получило большое внимание, начиная примерно с

декабря прошлого года и в течение первых нескольких месяцев этого года.

Как и в фишинге, здесь злоумышленник получает похожее доменное имя, зарегистрированное в неправомерных целях. Иногда они получают доменное имя, которое может выглядеть как пакет программного обеспечения, или другой надежный бренд, или какая-то услуга. Но вместо того, чтобы использовать его в электронной почте, они обращаются к провайдерам поисковиков и покупают рекламу.

В данном случае, который вы видите здесь на экране, это пришло от Abuse CH. Я взял это из их Твиттера. В данном случае злоумышленник притворяется, что у него есть сайт, связанный с законным почтовым клиентом Thunderbird. Это программное обеспечение, которое нравится многим людям. Но очевидно, что они делятся им не только по доброте душевной.

Если бы вы перешли на его рекламный сайт, расположенный вверху, вы бы получили это программное обеспечение плюс вредоносное ПО на свой компьютер - в данном случае IcedID. Это разновидность банковского троянца. Если он был установлен на вашем компьютере, то в конечном итоге он будет перехватывать, когда вы входите в свой банк, красть эти учетные данные и затем пытаться опустошить счета.

Новая тенденция интересна тем, что она все еще зависит от злонамеренно зарегистрированных доменов. Является ли это фишингом как таковым? Скорее всего, нет, потому что здесь нет связи с электронной почтой. Но конечный результат все тот же. Я обращаю на это внимание, во-первых, потому что это новое явление;

во-вторых, потому что оно напрямую связано с DNS; в-третьих, потому что я считаю важным признать, что мы должны быть немного более гибкими и проворными в реагировании на реальные ситуации в мире и быть готовыми включить эти новые тенденции в наши идеи о том, что мы можем решить.

Но, как и раньше, ответственные регистраторы, которые принимают меры против злонамеренно зарегистрированных доменов, также занимаются этим вопросом, и это хорошо. Следующий слайд. И это будет мой последний слайд.

Я просто хочу еще раз подчеркнуть этот момент. По-английски мы бы сказали "бить мертвую лошадь". Но фишинг является общепризнанным среди всех членов нашего сообщества здесь, в ICANN, как злоупотребление DNS. Кроме того, как я только что узнал из наших последних отчетов, в настоящее время это самый распространенный вид интернет-преступлений. И фишинг позволяет совершать многие другие преступления.

Оперативные действия против злонамеренно зарегистрированных доменов и меры поощрения, которые мы можем обеспечить с помощью нашей политики, имеют значение. Это влияет на то, что мы видим. Это мой главный вывод, и я ценю ваше внимание.

Я думаю, что теперь, когда Бертран здесь, рядом со мной, и готов, мы можем передать ему слово.

MANAL ISMAIL: Да, пожалуйста, Бертран. Продолжайте. И большое спасибо Интернет и юрисдикции за то, что вы всегда поддерживаете связь с

GAC и информируете нас о работе, которую вы проводите в отношении злоупотреблений DNS, что, безусловно, является темой, представляющей большой интерес для GAC. Спасибо.

BERTRAND DE LA CHAPELLE: Большое спасибо, Манал. Мне очень приятно вернуться в GAC, потому что много лет назад я был здесь в качестве представителя Франции, в том числе в качестве заместителя председателя GAC. Я вижу несколько знакомых лиц с тех времен. Мне очень приятно иметь возможность выступить здесь.

Я являюсь исполнительным директором Сети Интернета и политики юрисдикции (*Internet and Jurisdiction Policy Network*)- организации, соучредителем которой я стал 10 лет назад. И я очень рад возможности выступить здесь и поговорить об этих дебатах, которые оживляют сообщество ICANN в течение нескольких лет, и немного рассказать о том, над чем мы работаем, чтобы помочь дебатам развиваться дальше и продвигаться к решениям.

Сеть Интернета и политики юрисдикции - это... А Аджит Фрэнсис (Ajith Francis), который стоит здесь сзади, является директором по программам. Мы являемся мультистейкхолдерной инициативой, объединяющей правительства, компании, технических операторов, научные круги, гражданское общество и международные организации для решения юрисдикционных проблем в Интернете.

В частности, у нас есть - следующий слайд, пожалуйста, - три программы, я не буду подробно останавливаться на двух первых. Но одна из них, под названием "Домены и юрисдикция", посвящена вопросу о том, когда именно уместно действовать на уровне DNS для

устранения злоупотреблений? Существует контактная группа, которая работает уже более пяти лет, в нее входят около 40 человек из различных сообществ.

Я очень рад сказать, что Манал очень любезно, и другие люди здесь, включая Сюзан, активно участвовали в работе. Я особенно благодарен ей, учитывая большую нагрузку, которая на ней лежит, что она нашла время для участия. Это было важно.

В основном - следующий слайд, пожалуйста, - важно то, о чем мы здесь говорим, - как нам бороться со злоупотреблениями, существующими в Интернете? Эти злоупотребления чрезвычайно разнообразны. Презентация, представленная передо мной, показывает, что человеческая изобретательность абсолютно безгранична. Любой способ, которым мы можем использовать что-то не по назначению, будет использован не по назначению. Мы все это знаем.

Итак, главный вызов заключается в том, что в большинстве случаев - и это второй момент - это транснациональная проблема. Особенно интересно говорить об этом в GAC, потому что вы являетесь представителями правительств. Я был представителем правительства. И мы все знаем, что причина, по которой у нас есть проблемы с борьбой со злоупотреблениями в Интернете, заключается в том, что у нас нет инструментов сотрудничества между правительствами, чтобы действовать на транснациональном уровне. У нас есть международная архитектура, основанная на разделении суверенитетов, и сотрудничество крайне затруднено.

Одна из наших программ направлена на решение проблемы трансграничного доступа к электронным доказательствам. Это чрезвычайно проблематичный вопрос, и требуются годы для организации надлежащей правовой процедуры между странами для проведения расследований с использованием электронных доказательств. Таким образом, проблема, с которой мы сталкиваемся, заключается не только в том, что сеть глобальна, не только в том, что субъекты свободно работают через границы, но и в том, что инструменты, которыми мы располагаем для решения этой проблемы, неэффективны и не способствуют межправительственному сотрудничеству.

Следующий момент заключается в том, что для решения этих проблем необходимо лучше понять, как функционирует сам Интернет. Когда мы говорим о системе DNS, во многих кругах, с которыми вы, вероятно, знакомы, общаясь с коллегами, отсутствует понимание того, как функционирует эта архитектура. Если вы хотите понять, как связаться с владельцем домена, нужно знать, как функционирует WHOIS, что вы собираетесь найти регистратора и так далее. Это не так просто.

Следующий момент, который еще более важен, заключается в том, что я говорил о недостатке инструментов, но есть также вопрос компетенции. Операторы DNS — это всего лишь базовый союзник, предоставляющий доступ к доменным именам. У них нет никакой компетенции в том, чтобы исследовать, по сути, является ли что-то фишингом, является ли это вредоносным ПО, поэтому они полагаются на уведомителей. Еще хуже - я вернусь к этому позже -

когда мы говорим о злоупотреблениях, связанных с контентом. Как вам удается оценить законность контента в разных юрисдикциях?

Я затрагиваю вопрос о ресурсах, потому что расследование любого отдельного дела - а их может быть сотни тысяч - требует времени. Это относительно медленная и малоприбыльная отрасль.

В итоге, это проблема, которая является проблемой для всех. Это проблема для правительств, потому что вы беспокоитесь, вполне обоснованно, что злоупотребления не решаются. Это проблема для бизнеса, потому что он также является жертвой или несет бремя решения этих проблем. И это проблема для пользователей.

Итак, следующее, что нам нужно понять - следующий слайд, пожалуйста, - что-то базовое. Вы все знакомы с этим, но я хочу поделиться этим, чем я часто делюсь с людьми за пределами нашей собственной среды, потому что они не обязательно знают, как именно функционирует система. Итак, взаимоотношения между владельцем домена, регистраторами, регистратурами и пользователями; запросы, которые идут от одного к другому; и роли, которые различные участники играют в том, чтобы Интернет, который мы знаем, функционировал так, как мы хотим, чтобы он функционировал.

Это архитектура, на которой я не буду останавливаться подробно. Я хочу сказать, что существует только четыре действия, которые операторы DNS могут предпринять в отношении доменных имен.

Первое - следующий слайд, пожалуйста, - вы можете заблокировать домен. В принципе, вы не можете изменить информацию, предоставленную владельцем домена. Вы не можете передавать,

удалять, изменять. И вы не можете изменить ни сервер, ни IP-адрес, который был указан. Важно отметить, что это действие не делает контент недоступным. В частности, вы можете заблокировать его. Это полезно для последующего расследования. Но это ничего не меняет в функционировании.

Второй элемент - вы можете удерживать. В этом отношении вы берете доменное имя, удаляете из публичного файла зоны TLD, и домен не резолвируется. Вы также не можете изменить информацию, касающуюся сервера. Но и здесь система продолжает функционировать. Если вы используете IP-адрес, вы по-прежнему можете иметь доступ к элементу.

Третий элемент - перенаправление. Он часто используется для синкхолинга определенного доменного имени, когда вы хотите провести расследование. По сути, это редактирование файла зоны для перенаправления на другой сервер для наблюдения за поведением, определения жертв и тому подобных вещей.

Четвертый элемент - передача, когда вы передаете доменное имя другому регистратору. Это может произойти, когда регистрация была выполнена неправильным образом у одного конкретного регистратора. Но по какой-либо причине возникает интерес передать ее, например, регистратору последней инстанции, в чем очень активно участвует Бенедикт Аддис (Benedict Addis).

Следующий слайд важен, потому что это четыре вещи. Вы можете удалить, но я не буду подробно останавливаться на удалении, потому что это не рекомендуемое действие по разным причинам. Главный вопрос заключается в том, являются ли действия на уровне

DNS, включающие только эти четыре вещи, правильным инструментом для борьбы со злоупотреблениями?

Ответ - да, в некоторых случаях, и нет - в других. Это не идеальная панацея. Это не совсем то, что некоторые люди за пределами нашего сообщества склонны считать своего рода большой панелью управления. Как будто у вас есть проблема на доменном имени или прикрепленном к доменному имени, вы просто щелкаете выключателем, и проблема исчезает. Это не так, но все же в некоторых случаях полезно иметь соответствующие действия.

Итак, ключевые проблемы, или ключевые вопросы, заключаются в следующем. Во-первых, это инструмент, который рассматривает не только услугу доступа к сайту с доменным именем, но и множество вспомогательных услуг. Это может быть электронная почта, передача файлов и другие вещи. Так что это очень тупой инструмент.

Во-вторых, он имеет глобальное влияние. Он охватывает весь мир. Вы не способны действовать тонко. Вы не гео - блокируете приостановку доменного имени. Здесь интересно, потому что вы можете рассматривать это как особенность или баг. Если это баг, то он имеет глобальное влияние, поэтому он не гранулированный. Но в связи с тем, о чем я говорил ранее, нам не хватает инструментов для международного сотрудничества. Наличие чего-то, что имеет глобальный эффект, полезно в некоторых случаях.

Далее, как я уже сказал, вы по-прежнему можете получить доступ к большинству услуг через IP-адрес. Далее, вы находитесь в ситуации, когда операторы DNS являются частью более крупной экосистемы. Нам необходимо учитывать общую архитектуру, включая хостинг-

провайдеров, интернет-провайдеров и других участников, которые также могут иметь свои действия. Действовать на правильном уровне — вот что важно.

Следующий момент: в настоящее время в соглашениях об аккредитации регистраторов и регистратур с ICANN есть обязательство иметь точки контакта по злоупотреблениям и проводить расследования, но есть ограниченное количество обязательств, которые разъясняют, что действительно требуется и что действительно необходимо.

Это приводит к ситуации, которую мы наблюдали в течение длительного периода времени, а именно: в ICANN в течение многих лет велись и ведутся затяжные дебаты вокруг самого слова "злоупотребление DNS" и определения того, что оно означает. Люди занимали очень разные позиции в этом отношении. В связи с этим в течение нескольких лет проводились многочисленные заседания. Критика между различными группами интересов по поводу того, каким должно быть определение - таким или таким. И даже напряженность внутри различных групп относительно того, какие действия следует предпринимать или не предпринимать.

Это не значит, что они злоумышленники. Мы знаем, что есть злоумышленники. Есть субъекты, которые более ответственны, чем другие. Но очевидно, что здесь не было возможности прийти к консенсусу. В результате возникло чувство разочарования.

Суть в том, что если вы зададите неправильный вопрос, то вряд ли получите правильный ответ, а это требует переформулировки проблемы. Переформулировка, следующий слайд: реальный вопрос

заключается в том, когда уместно действовать на уровне DNS для борьбы со злоупотреблениями в Интернете? Я думаю, что это формулировка, с которой все могут согласиться как с правильной формулировкой, учитывающей различные элементы.

Следующий слайд... В рамках такой переформулировки мы долгое время работали с контактной группой, о которой я упоминал ранее, и сузили понимание злоупотреблений DNS, которые мы в свое время называли техническими злоупотреблениями. Но с помощью некоторых действующих лиц мы пришли к выводу, что злоупотребление DNS следует рассматривать как эти пять вещей: распространение вредоносного ПО, ботнеты, фишинг, фарминг и спам в той степени, в которой он используется в качестве механизма доставки вышеперечисленного.

Вы можете найти более подробную информацию об определениях этих пяти вещей сначала в оперативных подходах, которые I&JPN подготовила в апреле 2019 года. Это привело к включению этих определений злоупотребления DNS в Концепцию борьбы со злоупотреблениями, которая была подготовлена определенным количеством участников сообщества в декабре 2019 года, а затем в отчет SSAC 115 в 2021 году, в который было включено это определение злоупотребления DNS.

Возможно, это не идеальное определение, но оно является очень важным элементом, позволяющим провести различие между этим, что мы можем назвать злоупотреблением DNS, которое, как понимает каждый участник, имеет основания для расследования и находится в компетенции операторов, и злоупотреблениями, связанными с контентом, которые я рассмотрю позже.

В этом контексте мы подготовили - я не буду вдаваться во все подробности - набор инструментов в 2021 году, который я советую вам посмотреть в Интернете, чтобы помочь операторам DNS, уведомителям и законодателям или правоохранительным органам понять различные параметры и элементы руководства для объединения и совместной работы.

На следующем слайде упоминается важный элемент, который заключается в том, что в борьбе с любым видом злоупотреблений существует рабочий процесс, состоящий из четырех элементов. Первый - это идентификация самого факта злоупотребления. Оно может исходить от уведомителей или от самих операторов. Второй - оценка этого злоупотребления. Действительно ли оно оправдывает действия на уровне DNS?

Третий - какие действия следует предпринять из четырех перечисленных мною? И пятый - это то, что мы еще не обсуждали, но это часть общей картины, а именно: каковы пути обращения в суд, когда есть решение, которое было принято и которое должно быть изменено по какой-либо причине. Ошибки могут случаться.

Не слишком углубляясь, для каждого из этих этапов мы разработали определенное количество вещей, например, более четкое определение типов злоупотреблений. Упоминание элементов, касающихся того, что должны делать уведомители с точки зрения надлежащей осмотрительности, чтобы задокументировать эти элементы. Недостаточно просто бросить уведомление без каких-либо устойчивых доказательств. Каковы условия для уведомления владельца домена, особенно в случае взлома сайтов.?

При оценке возникает ключевой вопрос: каковы пороговые значения, критерии для действий? Когда необходимо достичь порога? И выбор действий. Есть разные типы действий, как я уже говорил. И есть документ, который точно объясняет рисунки, которые я показывал вам раньше. Наконец, что касается обращения в суд, есть вопрос о каналах обращения и элементах, касающихся прозрачности.

Это процесс. Все, что связано с расследованием попыток исправить ситуацию со злоупотреблениями, проходит через различные этапы, которые предполагают сотрудничество между различными субъектами. Если я перейду к следующему слайду, то в этом контексте контактная группа подготовила ряд документов, которые, я надеюсь, будут полезны для вас как для сообщества, а также полезны для общих дебатов.

Первый из них касается того, что должны содержать уведомления? Каковы компоненты уведомлений, подтверждающих доказательства? Второй - каковы типы уведомителей? Одинаково ли быть уведомителем в отношении изображений сексуального насилия над детьми или, например, в отношении нарушения коммерческой торговой марки?

Далее, как я уже сказал, какова должна быть комплексная проверка, которую должны пройти уведомители, чтобы бремя проверки не лежало полностью на операторах? Какое взаимодействие может быть между доверенными уведомителями? Каковы механизмы работы доверенных уведомителей?

Здесь я хочу сделать пояснение. Никто не может сам по себе сказать: "Я - доверенный уведомитель". В лучшем случае, вы можете сказать: "У меня есть опыт в этой конкретной области, что делает меня экспертом-уведомителем". Отношения с доверенным уведомителем — это двустороннее признание. Вы можете быть доверенным уведомителем для одного оператора, но не для других. Это важное различие, и нам нужно больше работать над понятием уведомителей.

В специальном документе рассматривается вопрос о ботнетах. У меня нет времени вдаваться в подробности. Но есть очень важный вопрос, который называется алгоритмически генерируемые домены. Нахождение лучшего сотрудничества между правоохранительными органами, ICANN и операторами DNS относительно алгоритмически генерируемых доменов является очень важным элементом. Я думаю, что этот документ помог немного продвинуть дискуссию вперед.

Наконец, что касается фишинга и вредоносного ПО, мы работали с контактной группой над составлением четкого графического рабочего процесса по распределению ролей на различных этапах между регистратурами и регистраторами? Каковы каналы передачи информации и так далее?

Я очень рад упомянуть об этом здесь, потому что Грэм Бантон (Graeme Bunton) находится здесь в углу, и некоторые из вас видели его раньше. Это привело к двум замечательным инициативам, которые, как я очень рад, были построены на фундаменте работы, проведенной в I&JPN, - созданию Института злоупотреблений DNS благодаря помощи PIR и созданию в этом контексте того, что мы

обсуждали в контактной группе, - интерфейса для сообщения о злоупотреблениях, который теперь называется NetBeacon.

CleanDNS был ... Джефф Бедсер (Jeff Bedser) сыграл важную роль в том, чтобы это произошло. Брайан Симболик (Brian Cimbolic) находится рядом с ним для PIR. Брайан фактически является координатором контактной группы, которую мы имеем в I&J. Эта работа удивительна для меня, потому что она является результатом пятилетней работы, ведущей к очень конкретному элементу, чему-то оперативному, что не является просто обсуждением или бумагой. Это действительно что-то действующее. Большой поклон им, которые несут факел вперед.

Это важно, потому что, кроме того, это привело также к дискуссиям, которые происходят здесь во время этой конференции ICANN76 относительно улучшения Соглашения об аккредитации.

Итак, я закрываю эту часть, и у меня есть очень короткая часть после этого. Речь идет о злоупотреблении DNS, понимаемом как пять элементов, о которых мы говорили. Следующий слайд, пожалуйста. Я думаю, что, в целом, среди ответственных лиц существует согласие, что злоупотребление DNS, понимаемое таким образом, — это то, что действительно является чем-то, что в целом оправдывает действия на уровне DNS, когда есть обоснованные доказательства, если только сайт не был взломан или есть другие вещи. Но в целом мы видим движение в положительном направлении в сторону реализуемого сотрудничества.

Последняя часть, которую я хочу затронуть, и которая в данный момент находится в стадии разработки, это вопрос о

злоупотреблениях, связанных с контентом, который гораздо сложнее, потому что здесь изображение немного зеркальное. Вообще говоря, уровень DNS не является подходящим местом для решения проблемы злоупотреблений, связанных с контентом, по многим причинам, включая тот факт, что он недостаточно детализирован. Трудно иметь что-то, приспособленное для борьбы с незаконными действиями в том или ином регионе.

Компетентность в оценке того, есть ли злоупотребление, значительно отличается. Это не техническая вещь, которую знают операторы. И вообще говоря, это неэффективный инструмент, потому что в большинстве случаев контент остается доступным.

Но, тем не менее, существует определенное количество ситуаций, которые являются достаточно исключительными, чтобы оправдать действия на уровне DNS, когда они встречаются. И в оперативных подходах, которые мы подготовили в 2019 году, перед глобальной конференцией, которую мы организовали в Берлине, есть четыре элемента, очень условно, которые можно принять во внимание, чтобы предположить или оценить, когда уместно действовать на уровне DNS в случае злоупотребления, связанного с контентом.

Насколько общепризнанно в мире, что данный контент является незаконным? Здесь у вас есть полная градация между вещами, которые, например, в одной крайности - CSAM, и вещами, которые чрезвычайно разнообразны с точки зрения законодательств по всему миру. Большое разнообразие в том, что является незаконным, а что нет. Доля сайта, отведенная под нарушающий права контент. Преднамеренность или недобросовестность владельца домена или оператора сайта. А также, были ли исчерпаны другие уровни для

обращения к оператору сайта, владельцу домена или хостинг-провайдеру.

Я не останавливаюсь на этом, но важно действительно провести различие между этими двумя категориями вещей. Обе они важны, но их нельзя рассматривать одинаково. Одна из больших проблем заключается в том, что у нас нет места для обсуждения этой второй проблемы. ICANN является подходящим местом для обсуждения вопроса о злоупотреблении DNS в том виде, в котором мы описали его ранее. Но было очень ясно, что, согласно мандату - и сообщество полностью согласно с этим — это не место для обсуждения злоупотреблений, связанных с контентом. В блогах постоянно появлялись сообщения о том, что "ICANN не является полицией контента" и т. д. И это совершенно понятно.

Проблема в том, что мало где еще это можно обсудить. Именно по этой причине в мае прошлого года, в 2022 году, значительная часть людей, участвовавших в контактной группе I&J, попросила нас стать тем местом, где можно было бы обсудить злоупотребление контентом веб-сайтов в тех исключительных обстоятельствах, найти пороговые значения, критерии и механизмы.

Это то, к чему мы приступили в этом году. Это предварительная работа. Это только начало. Но я думаю, что для этого сообщества GAC важно иметь полную картину и понимать, что ICANN действительно движется вперед на основе работы, которую мы коллективно проделали по вопросу злоупотребления DNS. Она не идеальна, и ее нужно реализовать, и ее нужно укрепить. Но она действительно продвигается вперед в этом отношении - лучшая ясность, лучшие механизмы и лучшее сотрудничество.

Что касается злоупотреблений, связанных с контентом, хотя это и не относится к ICANN, мы, I&JPN, продолжаем эту деятельность в отношении следующих элементов, которые представлены на следующем слайде. Во-первых, уровень DNS для злоупотреблений, связанных с контентом, задействуется либо потому, что есть абсолютная причина обратиться непосредственно туда, либо потому, что это последнее средство после исчерпания других уровней в общей системе. И вопрос о том, как связаться с оператором сайта, владельцем домена, хостинг-провайдером? Каков канал передачи разрешения проблем на более высокий уровень — это первый вопрос.

Второй элемент - как сформулировать пороговые критерии. Для примера можно сказать: "Весь сайт должен быть посвящен или уже посвящен нарушающему права контенту или деятельности". Или вы можете сказать: "На сайте нет другого законного контента, кроме этого". Или вы можете сказать: "Намерение оператора сайта состоит в том, чтобы делать то-то и то-то". Формулировки имеют значение, и мы содействуем этим обсуждениям.

Наконец, интересным является понятие достижимости. В тот момент, когда мы говорим, что существует канал передачи разрешения проблем на более высокий уровень, как отправить уведомление и как связаться с владельцем домена, или оператором сайта, или хостинг-провайдером, если на то пошло? Это то, что мы собираемся изучить более подробно, потому что четкого эквивалента WHOIS для хостинг-провайдеров не существует. Найти, где на самом деле размещен конкретный сайт, немного сложнее, чем просто узнать, кто является его регистратором.

Наконец, я упомянул о соглашении о доверенном уведомителе. Это чрезвычайно важный момент, потому что особенно для злоупотреблений, связанных с контентом - даже больше, чем для фишинга, но для злоупотреблений, связанных с контентом - не будет никакого решения без сотрудничества между тремя категориями участников - правоохранительными органами, уведомителями различных видов, которые должны наращивать свой потенциал и доверие, и операторами DNS в рамках существующих соглашений.

В качестве каламбура для тех из вас, кто помнит формулировку подтверждения обязательств между NTIA и ICANN в былые времена, я считаю, что существует рамочная концепция, которая представляет собой взаимное подтверждение обязательств. Нам необходимо иметь механизмы, которые объединяют уведомителей, обладающих компетенцией и процедурами надлежащего процесса, правоохранительные органы, способствующие сотрудничеству, и операторов для рассмотрения случаев, когда целесообразно действовать на уровне DNS.

Я хочу подчеркнуть, что то, о чем мы здесь говорим, не относится к регулированию крупных платформ. Это не Facebook. Это не Twitter этого мира. Вы не станете требовать удаления Facebook.com, потому что в одной из подгрупп, которая там находится, есть какой-то контент. Но когда кто-то создает сайт под доменным именем со злым умыслом, необходимо найти этих людей и прекратить эту возню: просто остановить здесь, потом остановить там, и перейти к поимке людей, которые на самом деле занимаются этим, — вот то важное сотрудничество, которое необходимо.

В итоге я хочу сказать, что это общая ответственность. Это то, что требует сотрудничества между различными субъектами. Девиз "Интернет и юрисдикция" - "Обеспечение сотрудничества между различными заинтересованными сторонами". Мы делаем это, способствуя формированию определенного количества соглашений. Мы очень рады, что это привело к прогрессу в среде ICANN. И это единственный способ, которым мы можем решить эти вопросы.

У вас на слайдах есть ряд... Нет, здесь должен быть слайд раньше. Он исчез. Я его восстановлю. Есть слайд со всеми связями и ссылками на документы, которые я представил. На последнем слайде - мои контактные данные и контакты Аджита Фрэнсиса (Ajith Francis), если вы захотите поговорить с нами об этом после. Большое спасибо за возможность провести презентацию.

MANAL ISMAIL: Большое спасибо, Бертран, за очень тщательную, хорошо структурированную и информативную презентацию. Прежде чем передать слово нашим ведущим по теме из GAC, я хочу отметить очень терпеливую руку, поднятую в Zoom от Ирана. Вы хотите выступить первым? Хорошо. Кавусс, секундочку. Крис, а затем я предоставлю вам слово. Извините,

CHRIS LEWIS-EVANS: Спасибо, Манал. Я как раз хотел предложить. У нас было довольно много выступлений, довольно много мы говорили. Может быть, если у вас есть какие-либо соображения или вопросы к нам по последней паре презентаций, их можно задать сейчас. Затем мы рассмотрим текущую деятельность сообщества ICANN и соображения по поводу

формулировок Канкунского коммюнике. Здесь тоже будут вопросы. Но, возможно, просто по последним двум презентациям, которые мы сделали, некоторые вопросы и размышления были бы полезны сейчас. Спасибо.

MANAL ISMAIL: Большое спасибо, Крис. Кавусс, что-нибудь по первой части заседания, либо по темам, либо к Бертрану? Пожалуйста, вам слово.

KAVOUSS ARASTEH: Большое спасибо, Манал. Позвольте мне выразить искреннюю признательность всем присутствующим на подиуме. Это была, на мой взгляд, одна из самых интересных дискуссий, которые мы проводили о злоупотреблении DNS. Хотя я не хочу проводить сравнение между разными, но последняя часть, для меня, была очень интересной.

Как я уже говорил вчера, у нас есть проблемы. И мы решили эти проблемы. Что я рекомендую, во-первых, уважаемый председатель, вы и Нико, будущий председатель GAC, нам нужно внести в повестку дня GAC на следующей конференции больше времени для этой темы. Невозможно поверхностно прийти к чему-то и не вникнуть в суть проблемы, как мы это сделали сегодня, чтобы понять, что это такое. Есть много вещей [которые нужно иметь]. Я не знаю. У нас сейчас нет времени, чтобы объяснить. У меня есть некоторые предложения. Я не знаю, что вы мне предложите. Но есть путь вперед.

Но я думаю, что хочу затронуть только один из пунктов. Уважаемый друг с правой стороны подиума упомянул о межправительственном сотрудничестве. Это обсуждалось много лет. Это не вопрос ICANN, потому что ICANN не является межправительственной организацией, и GAC не является межправительственной организацией. GAC - это Правительственный консультативный комитет. Правительства являются межправительственными. Они есть в других местах, но не здесь.

И я прошу прощения. Я [очень откровенен со всеми]. Много раз мы хотели рассмотреть этот вопрос, межправительственное сотрудничество. Некоторые правительства выступали против этого, говоря, что киберпреступность - это национальный вопрос и не должен рассматриваться на международном уровне. И они говорили, что любое межправительственное сотрудничество может быть полезным, если [заключить] договор. А договор по этому вопросу невозможен.

Поэтому давайте разберемся в глубине ситуации, не на этом заседании, потому что мы находимся в конце заседания. Давайте, уважаемый председатель GAC, если это возможно, мы обсудим вопрос немного дальше, чтобы посмотреть, что мы можем сделать. Было поднято много хороших вопросов. То, что до сих пор поднималось, это в основном проблемы. Но решения все еще не предложены. Это важно. Иногда, я бы сказал, не очень легко, но легко поднять проблему. Но гораздо сложнее предложить решения. Где же решения?

Мы должны использовать наиболее прагматичный подход, а не законодательную часть, чтобы посмотреть, что мы можем сделать.

Распределить их по категориям, по степени приоритетности, что мы можем сделать. Межправительственное сотрудничество, на данный момент, не так легко решить. Но есть много других вещей, которые нужно решать, и так далее, и так далее.

Мы получили сообщения из Великобритании и из США. Мы могли бы спросить всех членов GAC: "Есть ли у вас такой же опыт? Каков отчет? Сталкивались ли вы с ...?" Я сталкивался, но я никогда не сообщал. Я лично, по электронной почте много раз... Я вчера рассказывал. Там было [еще одно] сообщение, что [у них есть дипломатический автомобиль] с 10% скидкой. Я не стал открывать, потому что мой сын очень умный. Сказал мне: "Папа, не открывай ничего из этого. Не открывай. Если тебе пришло письмо по электронной почте, ты не знаешь отправителя, не открывай. Может быть, это не хорошо, не [неразборчиво]. Но не открывай это, потому что тебя могут сразу же...".

Есть и другие подходы. Некоторые провайдеры электронной почты обеспечивают двойную защиту, что если ваш пароль и т.д. и т.п. будет кем-то похищен, помимо вашего рабочего стола или оборудования, никто не сможет воспользоваться этим, потому что они используют второй подход - вторую защиту. Поэтому мы должны дать людям несколько хороших советов в качестве предварительной меры предосторожности. Что это за меры, которые хотя бы уменьшат количество этого? Так что это то, что мы должны обсудить.

Есть много других вопросов, но у меня нет времени. Так что извините, если я [неслышно], но это все. Спасибо.

MANAL ISMAIL: Большое спасибо, Иран. Если вы позволите, Крис, у нас есть еще две просьбы о предоставлении слова, и, возможно, вы сможете немного отреагировать. У нас осталось всего 20 минут, и у меня есть Демократическая Республика Конго, а затем США. Пожалуйста, продолжайте. Демократическая Республика Конго, вам слово.

BLAISE AZITEMINA FUNDJI: Большое спасибо. Спасибо всем выступающим. Я бы очень хотел, как и Кавусс, отметить, насколько важна эта презентация. С точки зрения правительства, для большинства правительств, и в основном из Африки, я думаю, что ожидания нашего правительства от участия делегата в GAC в основном направлены на борьбу с такого рода злоупотреблениями.

Мой вопрос или комментарий будет в основном касаться, конечно, очевидно, что название или тема здесь - злоупотребления. Но я хотел бы спросить, есть ли какие-либо действия, которые могут быть предприняты правительствами для предотвращения. Конечно, мы говорим об исправлении, о излечении. Но, как вы знаете, во французском языке мы говорим: "Il vaut mieux prévenir que guérir". Есть ли какие-то действия, которые ICANN может посоветовать.

Конечно, мы говорим о вопросах кибербезопасности, где задействован суверенитет государств. Но даже с точки зрения рекомендаций, в основном для корпораций и в основном для правительств, каковы рекомендации? Как мы можем предотвратить это?

Мы видели несколько презентаций от ФБР и в основном из опыта Великобритании. Я понимаю, что есть некоторые исследования. Есть

некоторые статистические данные, которые могут помочь понять, почему мы имеем такого рода злоупотребления. Мы знаем, что со стороны конечных пользователей это в основном фишинг. Это рассылка электронной почты, взлом паролей. Но для корпораций и, в основном, правительств, есть ли какие-то действия, которые можно предпринять для предотвращения, а не ждать, пока злоупотребление исправится? Спасибо.

MANAL ISMAIL: Большое спасибо, Конго. У меня США и Франция, пожалуйста, очень коротко. Затем я передам слово Крису. США, пожалуйста, вам слово.

SUSAN CHALMERS: Спасибо, Манал. Я с удовольствием уступлю слово, чтобы ответить на вопрос нашего коллеги. Спасибо.

MANAL ISMAIL: Большое спасибо, США. У меня Франция, а затем я передаю слово вам. Вы согласны, Крис? Франция, пожалуйста, продолжайте.

JONAS ROULE: Прежде всего, позвольте мне поблагодарить всех участников дискуссии за их презентации. Для меня большая честь присутствовать здесь вместо моего предыдущего коллеги. Я просто хотел выступить, чтобы внести свой вклад в дискуссию. Я новичок в GAC, и у меня сложилось впечатление, что прежде, чем приступить к работе, я должен узнать больше о некоторых темах.

Во-первых, как новичок, я хотел бы изучить некоторые средства, чтобы понять, могу ли я что-то сделать для предотвращения внешних атак. Я чувствую, что выгодная цена, предлагаемая некоторыми субъектами, приводит к некоторым злоупотреблениям в DNS. Поэтому я хотел бы узнать, как мы могли бы работать, чтобы увидеть показатели продления доменных имен. Возможно, это поможет сообществу сделать что-то в этом направлении.

Мы знаем, какие субъекты действуют не легально. Поэтому, возможно, мы сможем раскрыть некоторые механизмы, которые они используют. Но некоторые трудности, которые мы наблюдаем, нуждаются в доказательстве. Я думаю, это то, что нам нужно. Спасибо за внимание.

MANAL ISMAIL: Большое спасибо, Франция. Я вижу, что Руанда подняла руку. Не могли бы вы говорить очень кратко, потому что у нас мало времени.

VINCENT MUSEMINALI: Большое спасибо. Я просто хочу поблагодарить докладчиков, участников дискуссии, которые представили презентацию отчета США и отчета Великобритании по киберпреступности. Просто чтобы получить некоторые разъяснения [неслышно] криптовалюты. Большинство людей сейчас сталкиваются с некоторыми проблемами, связанными с доменами, которые используют киберпреступления, [связанные] с криптовалютами. И эти домены иногда закрываются, и люди [неслышно] теряют свои деньги и инвестиции. И им [теперь] приходится делать последующие шаги в

отношении этих инвестиций. Я хотел бы узнать, как они сотрудничают с Интерполом. Спасибо.

MANAL ISMAIL: Большое спасибо, Руанда. Возвращаемся к вам, Крис. Извините, что поджимаю вас по времени, но я рада слышать коллег из GAC. Пожалуйста, вам слово.

CHRIS LEWIS-EVANS: Спасибо, Манал. Это точно так, и большое спасибо за ваш вклад. Я постараюсь довольно быстро подытожить некоторые из своих выступлений. Что касается вопроса по поводу рекомендаций, которые мы услышали и от Конго, и от Франции, то мы не будем их рассматривать здесь и сейчас. Есть много рекомендаций. Есть много вещей, которые вы можете сделать. Может быть, это может быть темой для семинара по наращиванию потенциала в будущем ICANN. Так что, возможно, GAC следует рассмотреть этот вопрос, потому что это должно быть немного более длительное заседание. Так что мы могли бы рассмотреть этот вопрос.

Затем, по поводу вопроса Ирана о проактивности: "Что мы можем сделать?". Я думаю, Бертран рассказал о нескольких способах. NetBeacon, определенно упомянутый как инструмент отчетности, является способом действия и способом борьбы с некоторыми из этих проблем. Это ведет к текущей деятельности, если мы можем перейти к этим слайдам. Мы расскажем о некоторых действиях, которые происходят в сообществе, поддерживающем некоторые из этих злоупотреблений DNS.

Что касается криптовалюты, то я думаю, что это также относится к словам Бертрана. Это может быть доставлено либо из фишингового электронного письма, где это попадает под злоупотребление DNS, либо это может быть проблема, связанная с контентом, где это попадает под механизмы.

Затем перейдем к деятельности сообщества. Здесь ведется большая работа. Регистратуры работают над добровольным обменом статистикой. Как мы видели с точки зрения правоохранительных органов, мы считаем, что это очень важно. Это дает нам общую картину. То же самое касается и регистратур, которые будут поддерживать эту работу.

Остается только упомянуть о следующем, а именно acidtool.com. Бертран сказал, что не существует инструмента для определения провайдеров хостинга и электронной почты. На самом деле, регистраторы создали этот инструмент, чтобы помочь людям определить правильный и верный пункт, в который нужно обратиться, чтобы предпринять эффективные действия. Мы слышали из презентации I&J, что принятие эффективных мер действительно важно. И определение правильного пункта, будь то реселлер, регистратор, регистратура или хостинг-провайдер, действительно важно.

Еще один призыв к NetBeacon, опять же, здесь, в качестве метода принятия мер. Это очень соответствует рекомендациям SSAC115. У нас была хорошая презентация от SSAC по этому вопросу, и, опять же, это упоминается в отчете I&J. Это все мероприятия, которые помогают смягчить те [рекомендации], которые происходят в настоящее время. Кроме того, Институт злоупотреблений DNS

делится результатами своей аналитической работы на основе данных, которые он собрал и увидел в рамках отчетности о злоупотреблениях DNS. Следующий слайд, пожалуйста.

Возможно, я говорю слишком быстро для переводчиков, поэтому я сейчас извинюсь и немного сбавлю темп. Малая группа GNSO по злоупотреблениям DNS также была очень активна. Я просто хочу отметить, что их выводы отражают некоторые из наших важных вопросов в Гаагском коммюнике о том, что любая будущая работа PDP по злоупотреблению DNS должна быть узкоспециализированной для получения своевременных и действенных результатов. Так что, как сказал Иран, любая работа, которую мы проводим в сообществе, должна быть целенаправленной, чтобы она могла произойти и произойти быстро. Я знаю, что иногда возникает разочарование по поводу того, что все происходит недостаточно быстро. Тогда, пожалуйста, следующий слайд.

Также в рамках полномочий ICANN у них есть команда OCTO, есть система DAAR. О ней мы также слышали в субботу, я полагаю, что это было в субботу, о том, как они анализировали данные 1 145 gTLD, что удивительно, как много их там было. Также есть, я думаю, 21 ccTLDs. Опять же, это просто лучшая картина, дающая большее понимание того, что происходит, чтобы можно было предпринять эффективные действия. Следующий слайд, пожалуйста.

Это просто напоминание об этом пути и о том, к кому обращаться. Это сложное пространство. Это диаграмма ICANN, так что большое спасибо. Я вообще не могу нарисовать ничего сколько-нибудь похожего. Мы слышим о том, что нужно обратиться к нужному

человеку, чтобы он смог предпринять нужные действия в нужное время. Конечно, с моей точки зрения, мы видим, что там, где мы можем это сделать, это также уменьшает вред. Поэтому способность понять, куда идти и куда быстро идти, действительно важна. Так что такие инструменты, как NetBeacon, ACID Tool, очень полезны.

На самом деле картина несколько сложнее. С правой стороны у вас есть владелец домена, а затем реселлер. Не всегда есть реселлер, а иногда их несколько. Таким образом, понимание этого очень важно для того, чтобы найти правильное место, куда нужно обратиться. Следующий слайд, пожалуйста.

Хочу отметить, что в ходе первой фазы работы над EPDP было рекомендовано, чтобы регистраторы создавали элемент данных о реселлерах для реселлеров, поддерживающих отношения с владельцем домена. Это важно, когда их несколько. Так, в ответе WHOIS в настоящее время есть поле реселлера, но оно не обязательно собирает все данные. И, как я уже сказал, для нас очень важно иметь возможность обратиться непосредственно к человеку, который может принять наиболее эффективные меры. Это также нашло отражение в обзоре CCT. Следующий слайд, пожалуйста.

И передаю слово Лорин. Я прошу прощения, что говорю быстро, но я хотела бы перейти ко второму блоку вопросов, если можно.

MANAL ISMAIL: Лорин, у нас уже есть просьба о предоставлении слова. Хотите, чтобы мы предоставили им слово первыми? Хорошо. Я вижу руку Великобритании. Найджел, пожалуйста, вам слово.

NIGEL HICKSON: Большое спасибо, госпожа председатель. Я буду рад, если первой выступит Лорин, а потом мы, возможно, вступим позже. Продолжайте, Лорин, пожалуйста.

LAUREEN KAPIN: Спасибо, Найджел. Я выступаю в качестве одного из сопредседателей Рабочей группы по общественной безопасности и одного из экспертов по этой очень важной теме. Можем ли мы перейти к следующему слайду?

Я рада, что заседание было интерактивным, даже до этого момента. Но было много обсуждений, перспектив и информации о том, что GAC хотел бы... Позвольте мне перефразировать. Было предоставлено много информации и перспектив. Сейчас мы находимся на той стадии, когда мы можем обсудить, что GAC хотел бы выделить в коммюнике, то есть потенциальные темы.

Во-первых, - и это относится к категории "если это стоит сказать, то стоит сказать много раз" - у нас есть продолжающиеся переговоры по договорам между регистратурами, регистраторами и ICANN. Опять же, вся цель этого процесса заключается в том, чтобы поднять уровень, то есть улучшить договорные обязательства в отношении принятия мер против злоупотреблений DNS. Именно обязательства, а не добровольные усилия. Цель этих обязательств - отразить обязательства, которые будут распространяться на всех. Это, надеюсь, охватит злоумышленников, а также даст ICANN еще больше инструментов, чем у нее уже есть, чтобы справиться с этими сценариями в отношении злоупотреблений DNS.

Опять же, это только первый шаг, и могут быть будущие шаги. Но это может быть важным моментом для GAC, чтобы признать и приветствовать, что эти усилия продолжаются и что они были предприняты по инициативе договорных сторон. Это проактивный шаг, и это всегда следует приветствовать.

Это первый из многих шагов, поэтому предполагается будущая работа по политике. Я хочу повторить один из комментариев моего коллеги из Ирана о том, что здесь очень важно расставить приоритеты и сосредоточиться, потому что именно так все и решается. И мы можем применить эти два руководящих принципа к любым PDP, которые не обязательно известны своими быстрыми и сфокусированными действиями, но они могут и должны быть такими в данном контексте. Кроме того, могут появиться возможности для проведения дополнительных переговоров между Договорными сторонами и ICANN.

Отметим, что в ближайшее время будет возможность для публичных комментариев, как только Договорные стороны опубликуют плоды своих трудов, чего мы с нетерпением ждем. Затем у GAC будет возможность решить, какой вклад он хотел бы внести. Следующий слайд, пожалуйста.

Эта проблема реселлеров также была обозначена. Как отметил наш коллега из Общества интернета и юрисдикции Бертран, это связано со злоупотреблением DNS, потому что это так важно. Так важно иметь возможность обратиться в нужную организацию, когда вы имеете дело со злоупотреблением DNS. Эта тема была предметом

вклада GAC во многих различных формах, связанных с итоговым отчетом CCT, а также совсем недавно с рекомендациями по Фазе 1 по регистрационным данным доменов. Следующий слайд, пожалуйста.

Теперь я возвращаюсь к моим коллегам по GAC, чтобы они высказали свои мысли и идеи о том, что может быть включено в коммюнике GAC. Я также отмечаю, что, поскольку времени мало, мы проводим заседания по подготовке коммюнике. Но сейчас самое подходящее время для того, чтобы получить предварительную информацию о том, что думают люди.

MANAL ISMAIL: Большое спасибо, Лорин. У нас Великобритания, Иран и Европейская комиссия. У нас есть три минуты, поэтому я надеюсь... Пожалуйста, будьте кратки. Великобритания, пожалуйста, вам слово.

NIGEL HICKSON: Да. Большое спасибо, Манал. Большое спасибо ребятам с подиума за то, что представили нам свои доклады. Это было исключительно полезное заседание, как отметили другие члены GAC. Если позволите, четыре очень быстрых замечания.

Первое — это подтвердить нашу позицию в отношении предстоящих переговоров по договору. Я настроен невероятно позитивно. Вчерашнее заседание с представителями регистраторов и регистратур я считаю превосходным. Мы с нетерпением ждем общественных консультаций. Мы не намерены вмешиваться в эти переговоры. Конечно, мы с нетерпением ждем новостей. И, как было

сказано вчера представителями, это первый шаг. Вполне возможно, что будут и другие инициативы - мини PDP или что-то еще - для рассмотрения злоупотреблений DNS.

Во-вторых, что касается коммюнике, мы, несомненно, будем обсуждать эти вопросы. Я думаю, что будет правильно, если в коммюнике мы очень четко обозначим, как мы приветствуем эти инициативы, но также укажем на эти рекомендации - рекомендации GAC по рекомендации 17 Анализа CCT и другие вопросы в отношении реселлеров, о которых уже говорилось, которые мы должны отметить, чтобы все сообщество понимало, что есть определенные действия, которые необходимо предпринять до следующего процесса SubPro. На этом я заканчиваю. Большое спасибо.

MANAL ISMAIL: Большое спасибо, Великобритания. Следующий у меня Иран, и я закрываю очередь после Японии, пожалуйста. Иран, вам слово.

KAVOUSS ARASTEH: Большое спасибо, Манал. Я обсуждал с некоторыми уважаемыми коллегами, включая вас, что вопрос злоупотребления DNS является основным вопросом текущей, ближайшей и долгосрочной перспективы ICANN. Это нечто важное. Но все - Правление, корпорация ICANN, членство и все остальные - изучают этот вопрос. Нет необходимости в каких-либо рекомендациях GAC по этому вопросу. Дайте людям отдышаться, обдумать, переварить вопрос и не давить больше, чем нужно. Они знают, что является проблемой.

С другой стороны, в вопросах, важных для GAC, первое, что мы должны упомянуть, что признание переговоров, проводимых в рамках Правления ICANN или ICANN и договорных сторон, регистратур и регистраторов, это хороший шаг - сказать об этом. И затем мы должны упомянуть, что нам нужен отчет о ходе переговоров на следующем заседании ICANN, ICANN77 в Вашингтоне, округ Колумбия - отчет о том, что происходит.

И мы ожидаем, что окончательный отчет будет либо 78, либо 79, либо 80, но с достаточными мерами, чтобы посоветовать правительству или GAC, как бороться, как противостоять, как упомянул мой коллега, или как противостоять этой ситуации, и увидеть многие другие элементы, которые были указаны в отчете Криса, и Лорин, и Габриэля - включив в него вопросы, важные для GAC.

И постараться подчеркнуть важность этого. Поработать над текстом, чтобы он был более ясным, более точным и кратким, а также попытаться [расставить точки] и сделать последующие действия. Но я предлагаю на данном этапе не включать ничего о злоупотреблении DNS в рекомендации GAC. Спасибо.

MANAL ISMAIL: Большое спасибо, Иран. У меня Европейская комиссия, затем Япония. И дружеское напоминание: пожалуйста, будьте кратки. Европейская комиссия, пожалуйста. Джемма, вам слово.

GEMMA CAROLILLO: Большое спасибо, Манал. Я уже дала высокую оценку презентациям в чате, поэтому не буду повторяться в интересах экономии времени. Если говорить очень кратко о пунктах и соображениях для коммюнике, как любезно спросила Лорин, то, конечно, мы согласны, что это отличный шаг. Переговоры, мы призывали к этому в течение долгого времени внутри GAC. Так что это то, что, безусловно, мы должны поддержать.

Что касается дополнительного содержания, мы могли бы добавить в раздел злоупотребления DNS в рамках важных вопросов. Они будут приняты, но, конечно, для дальнейшего обсуждения. Прежде всего, важность превентивных мер. Мы немного обеспокоены тем, что то, что мы слышали до сих пор, в основном касается реактивных мер. Но профилактика злоупотребления DNS действительно является ключевой с нашей точки зрения. Я слышала об этом ранее, также от одного или двух коллег. Затем, возможно, изучить вопрос о стимулах, который был поднят в очень хороших рекомендациях коллег из PSWG и т. д. местах.

И последнее, но не менее важное: в связи с тем, что сказал Найджел относительно следующего раунда gTLD, в целом, мы хотели бы убедиться, что предыдущая работа не забыта - в частности, в отношении разумных мер по предотвращению злоупотреблений DNS. Но GAC довольно сильно связал достоверность данных, достоверность регистрации доменных имен и злоупотребления DNS в коммюнике 71, 72, 73, и я уверена, что есть и другие. Так что это не для того, чтобы перечислить их, а просто для того, чтобы подчеркнуть, что мы хотели бы, чтобы работа, проделанная в отношении достоверности регистрационных данных и важности для

предотвращения злоупотреблений DNS, не была потеряна. Большое спасибо.

MANAL ISMAIL: Большое спасибо, Европейская комиссия. И последнее, но не менее важное, конечно же, Япония.

NOBU NISHIGATA: Большое спасибо, Манал, и сопредседателям PSWG. Спокойной ночи. В Японии уже ночь. Так что доброе утро, добрый день всем из Токио. Большое спасибо за организацию, которая провела сегодня это замечательное заседание.

Просто отвечая на презентацию Лорин о рассмотрении коммюнике. Япония хотела бы выразить поддержку ведущимся переговорам по договору, что очень приветствуется - текущий прогресс на данный момент.

Но, с другой стороны, Япония хотела бы поднять один вопрос и проблему в Соглашении об аккредитации регистраторов, в статье 3.18.1, которая касается необходимых действий регистратора по сообщению о незаконной деятельности. Японское правительство [сообщило] и знает, что некоторые регистраторы не предпринимают никаких действий или даже не реагируют на сообщения о незаконной деятельности от японских сторон. Именно поэтому японское правительство продолжает требовать улучшения текста или условий договора.

Есть некоторые доказательства со стороны японского правительства. Но, тем не менее, существует множество других доказательств,

подобных этому - аудиторский отчет ICANN или недавний отчет ICANN, GNSO, сторон. Так что в этом-то и дело, просто хочу сказать, что Япония с нетерпением ждет появления проекта отчета. Конечно, они рады обсудить его в межсессионный период, если у нас есть какой-то прогресс.

И, конечно, в заключение, я должен выразить огромную благодарность за предыдущее заседание, которое предоставило нам обновленную информацию о переговорах по договору. Так что мы готовы продолжить обсуждение - с удовольствием обсудим это с вами. Большое спасибо.

MANAL ISMAIL: Большое спасибо, Япония. И большое спасибо, Бертран, от Интернета и юрисдикции, Гейб, Крис и Лорин, ведущие по теме из GAC. И спасибо всем. Мы вновь соберемся здесь в 15:00 по времени Канкуна, 20:00 по Гринвичу, для двусторонней встречи с Правлением. Поэтому, пожалуйста, будьте оперативны. Спасибо.

[КОНЕЦ СТЕНОГРАММЫ]