DNS (с PSWG) (1/2)

RU

ICANN68 Виртуальный Форум по Формированию Политики – GAC: Смягчение злоупотреблений DNS (с PSWG) (1/2)
Понедельник, 22 июня 2020 года - с 11:30 до 12:30 MYT

GULTEN TEPE: Доброе утро, добрый день и добрый вечер. Это Гультен. Добро пожаловать на заседание GAC ICANN68 по злоупотреблению DNS GAC в рабочей группе по общественной безопасности. Мы не будем делать перекличку в интересах времени, но участие членов GAC будет отмечено и в приложении к коммюнике, и в протоколе GAC этой конференции ICANN68. Представителям и делегатам GAC предлагается указать свое имя, фамилию и страну или организацию, которую они представляют, в чате Zoom, точные записи об участии и облегчение очереди для комментариев и вопросов во время заседания. Было бы полезно, если вы хотите задать вопрос или сделать комментарий, введите его в чате, начав и завершив предложение словами <QUESTION> или <COMMENT> и, пожалуйста, сделайте их короткими, если это возможно. Синхронный перевод на заседаниях GAC будет включать все 6 языков ООН и португальский. И будет проводиться с использованием как Zoom, так и удаленной платформы для синхронного перевода, эксплуатируемой компанией Congress Rental Network. Информация о том, как установить и использовать это приложение, будет доступна в модуле чата.

Наша группа технической поддержки контролирует зал Zoom и является единственной, кто может включить микрофон после

запроса со стороны команды поддержки GAC. Если вы хотите выступить, пожалуйста, поднимите руку в зале Zoom, во время выступления обязательно отключите все ваши дополнительные устройства. С этим я хотела бы предоставить слово Манал Исмаил (Manal Ismail). Вам слово, Манал.

MANAL ISMAIL, ПРЕДСЕДАТЕЛЬ GAC: Большое спасибо, Гультен. И извините, мне потребовалось время, чтобы включить микрофон. Добро пожаловать всем на первое заседание GAC по смягчению последствий злоупотребления DNS, так как у нас запланировано 2 заседания по этой теме, одна перед сквозным заседанием сообщества, которая состоится позже сегодня, а вторая запланирована на завтра. Рабочая группа GAC по общественной безопасности будет руководить этим заседанием, которое запланировано на час. С 11:30 до 12:30 по времени Куала-Лумпур. С 3:30 до 4:30 UTC. Передаю слово Габриэлю и Лорин. Я не уверена, кто собирается начать.

GABRIEL ANDREWS: Здравствуйте, добрый день. Добрый вечер, доброе утро и счастливый день отца папам из западного полушария. Я вижу, у нас есть несколько тем, которые мы собираемся обсудить сегодня, если мы перейдем к повестке дня. Спасибо. Мы рассмотрим уроки, извлеченные из ответа на ситуацию с COVID 19. Это горячая тема, которая продолжается сейчас. Было много сторон, которые представили свою точку зрения, и мы расскажем об основных

моментах и расскажем о некоторых аспектах, с точки зрения правоохранительных органов и общественной безопасности.

У нас есть изменения и сделаем обзор последних событий, связанных со злоупотреблением DNS. Следующие шаги для GAC и соответствующие заседания ICANN68, посвященные злоупотреблениям DNS, которые могут представлять интерес для членов GAC. Следующий слайд, пожалуйста. Таким образом, за последние несколько недель было сделано несколько очень интересных презентаций об уроках, извлеченных из анализа регистраций доменов, связанных с COVID 19. Я кратко изложу некоторые ключевые моменты, которые, я надеюсь, мы точно извлекли из презентаций от регистратур национальных доменов и из отдела ICANN главного технологического директора. И мы поделимся некоторым опытом, который получила моя команда как правоохранительный орган США, работающий с подобными требованиями. Во-первых, регистратуры национальных доменов сообщают, что они предприняли активные шаги для включения мониторинга регистрации вместе с дополнительной проверкой личности, и они тесно сотрудничали с местными правоохранительными органами и командами. Кроме того, они сообщают о значительном всплеске регистраций, связанных с COVID, в рамках которых наблюдалась лишь очень небольшая криминальная активность.

Вы увидите это сообщение, повторенное сторонами, связанными договорными обязательствами и OCTO. Некоторые стороны, связанных договорными обязательствами, сообщили, что

аналогичным образом проводили дополнительные проверки регистрации доменов с использованием терминов или ключевых слов COVID, участвуя в рамках борьбы с злоупотреблениями, выявили необходимость принятия мер по борьбе со злоупотреблениями, которые могут привести к физическому ущербу, в доменах, связанных с COVID, из-за возможного злонамеренного использования. Кроме того, я обнаружил, как федеральный правоохранительный орган, что многие из подписавших рамки по борьбе со злоупотреблениями, действительно, предприняли заметные усилия для участия с правоохранительными органами, напрямую связавшись с нами и с партнерскими агентствами, и обнаружил, что большинство регистраторов отозвались на призыв и заслуживают признания. Как и прежде, стороны, связанные договорными обязательствами, сообщили, что наблюдали только очень небольшое количество подтвержденных злоупотреблений в очень большом количестве зарегистрированных доменов COVID. Как видно на этом слайде в небольшом тексте, вы увидите, что 70% таких регистраций были просто припаркованы и не использовались. Примерно 25% были использованы в законных или выгодных целях, и только 0,5% были замечены как зловредные.

Кроме того, были сообщения о черных списках доменов, разработанных сообществом или охранными фирмами, которые, возможно, оказывались чрезмерно агрессивными с некоторыми потенциально значительными ложными положительными среди них, под которыми я подразумеваю полезные сайты или

нейтральные сайты, ошибочно включенные в черный список. Некоторые стороны, связанные договорными обязательствами чувствовали разочарование, что были поставлены перед задачей определения того, что является или не является вредным, а не законным или даже того, кто направляет уголовные дела в пределах конкретной страны, в зависимости от типа наблюдаемого злоупотребления. Следующий слайд, пожалуйста. Анализ, проведенный отделом главного технологического директора ICANN, лично мне показался захватывающим. Они признали потенциальные возможности мошенничества и злоупотреблений, связанных с пандемией, и создали систему для выявления и передачи опасных доменов соответствующим сторонам.

Для этого они выполнили поиск по ключевым словам терминов, связанных с COVID, и схожие домены, известные как гомоглифы и т. д., на 16 языках, что является амбициозным, и проверили их на предмет уведомления о новой регистрации TLD. Они прошли ряд дополнительных этапов валидации, таких как сравнение с лентами новостей органов госбезопасности open source или с белыми списками ложных позитивов, например, в английском языке слово «коронация» содержит слово «корона», и, если было собрано достаточно информации, чтобы сделать убедительные выводы, они передали эти домены регистраторам и регистратурам. Выявив сотни тысяч регистраций доменов, связанных с пандемией, они в конечном итоге передали десятки доменов и сообщили о них. Итак, еще раз. Та же самая тема - там было очень много регистраций, в которых только небольшое количество было злоумышленными, и

это обзор высокого уровня, но если вы заинтересованы и пропустили первоначальный брифинг GAC от 15 июня, стоит его посмотреть. Вернитесь и посмотрите это заседание.

Следующий слайд, пожалуйста. Теперь я задержусь на нашей перспективе. И когда я говорю "на нашей", я хочу признать, что в Соединенных Штатах есть много наций и даже много агентств, которые проводили аналогичные процессы. Но безлично выступая от имени моего агентства как единого правоохранительного органа в Соединенных Штатах, то есть это будет основано на США, но я хочу признать, что мы были далеко не единственными, кто это делал. Поэтому очевидно, что правоохранительные органы будут заниматься преступниками, особенно теми, которые наиболее вопиюще стремятся использовать пандемию для мошенничества с электронной почтой, фишинга или распространения вредоносных программ, но мы приняли решение быть максимально прозрачными с жалобами и сообщениями, что мы получали. И поделиться как можно большей частью анонимной отчетности с регистраторами. Чтобы преследовать худшего из преступников, а не просто сидеть на отдыхе.

Наши исходные данные сильно отличаются от данных, которые используются ICANN или сторонами, связанными договорными обязательствами. Потому что вместо того, чтобы начинать с сотен тысяч регистраций доменов, мы начали с гораздо меньшего набора данных, по-прежнему в тысячах, но гораздо меньших случаев, когда домены сообщались нам как использовавшиеся для мошенничества, или распространения вредоносного ПО или

фишинга. Теперь, это включало в себя отчетность не только в оперативных отделах ФБР или партнерских агентствах, таких как FTS или даже в интернет-центре по преступлениям и жалобам IC3.GOV, но и в том, что мы стремимся сообщать о преступлениях в Интернете, но это включало в себя ценные данные от партнеров из частного сектора. Такие партнеры, как Microsoft, которые управляют крупной службой веб-почты и в режиме реального времени проверяют каждую утечку, отправленную через их службу веб-почты, и направляют нам те из них, которые соответствуют ключевым словам COVID и, как полагают, использовались при фишинге или распространении вредоносных программ.

Конечно, используя с разрешения здесь. Лаборатории Fisht, используемые с разрешения, также поделились с нами ценным реальным использованием слов. Это сделано для того, чтобы подчеркнуть, насколько партнерство, что борется с киберпреступностью, это партнерство между должностными лицами в сфере общественной безопасности и специалистами по кибербезопасности в частном секторе, и я хотел бы подчеркнуть, насколько ценно для нас иметь [неразборчиво], когда мы корректируем жалобы, мы беспокоились по поводу ложных позитивов. Таким образом, мы читали каждую жалобу и, когда мы получали отзывы от регистраторов, которым мы передавали данные, мы стремились включить все больше и больше информации, которая могла бы оказаться полезной регистраторам для принятия решения о том, какие действия могут быть

оправданы. Мы снова использовали помощь партнера из частного сектора в этом случае риска, который я запрашиваю.

Чтобы обеспечить безопасные снимки или снимки экрана, чтобы регистраторам не нужно было бы самим посещать эти рискованные сайты. Мы использовали VirusTotal и доменные инструменты. ... для удобства просмотра и проверенных кодов EPP, чтобы свести к минимуму количество рефералов для уже отключенных сайтов. И мы старались, где это возможно, включать образцы самой анонимной жалобы. Когда мы передали эти домены еще одну вещь, которую мы сделали, что было необычно для нас, мы отправили регистраторам вместе с ними письма о сохранении, с просьбой, чтобы вся информация должна быть сохранена. И я собираюсь рассказать вам позже о том, почему это письмо о сохранении мы считали необходимым. Потому что это своего рода болевая точка для нас. Следующий слайд, пожалуйста. Итак, цифры. Мы передали 1349 доменов по состоянию на 12 июня. Теперь это число могло быть намного выше, но опять же, мы хотели минимизировать количество ложных позитивов. И отправили только домены с достаточным количеством вспомогательной информации, на основании которой, как мы думали, будут действовать регистраторы. Мы отсылали эти домены еженедельно. Вернитесь, пожалуйста. Спасибо.

Он еще нужен. Мы отправляем эти ссылки еженедельно. И наш пик произошел 17 апреля или около того с более чем 350 доменами, переданными на этой неделе. Теперь для сравнения следующий слайд, к которому вы можете перейти, украден из презентации

главного технического директора ICANN, и вы увидите, что их пик регистрации доменов по теме COVID, не используемых, но регистрации произошли 25 марта или около этого. Наш, опять же, был 17 апреля. Таким образом, наша кривая, похожая по форме, похоже, следовала за OCTO 3 недели, и было бы заманчиво сделать из этого вывод, что может пройти около 3 недель, чтобы домен перешел от регистрации злоумышленником к использованию преступником, и был замечен жертвой, и о нем сообщили нам. Мы его рассмотрели и отправили. Я уверен, что ученые в аудитории бросят в меня помидоры из-за этого вывода, но это заманчиво. Это подчеркивает, что ссылки правоохранительных органов ценны только потому, что они приносят отчеты об использовании в реальном мире, они всегда будут реагировать.

И редко такие ссылки будут предупредительными. Это просто не та роль, которую мы в состоянии оказывать, упреждающие усилия почти всегда должны быть в руках самих регистраторов. Следующий слайд, пожалуйста. По количеству регистраторов, которым мы отправили ссылки. 104 на 12 июня. Здесь показана первая десятка с очень длинным плоским хвостом справа от экрана. Это не обвинительный акт GoDaddy. Мне нужно прояснить это. Регистратор GoDaddy был среди самых открытых и отзывчивых на протяжении всего процесса. Многие другие были открытыми и полезными в наших беседах.

У них просто большая доля рынка, и я не думаю, что есть что-то кроме этого факта. Домены, которые мы сделали, стоит упомянуть, что они выходили за рамки просто случаев фишинга или

распространения вредоносного ПО, но включали в себя сообщения о мошенничестве, и я хотел бы привести один пример этого. Это пришло из нашего регионального отделения в Бостоне, который уведомил нас о том, что семья ветерана получает жестокие угрозы в их доме. Очевидно, кто-то продавал маски COVID онлайн и обманным путем указывал адрес компании как место жительства этого ветерана. Таким образом, клиенты, которые были недовольны тем, что заплатили за маски и так никогда их не получили, по ошибке направили этот гнев на семью этого ветерана, и, к счастью, регистратор, в этом случае Tucows, быстро отреагировал.

Очень быстро и учитывая угрозу физического вреда, мы приостановили действие домена. Именно такое реагирование мы высоко ценим, ценят наши коллеги из Бостона, и я уверен, что та семья. И это только один из 1300 ссылок, но мы ценим все случаи, когда регистраторы считали, что мы предоставили достаточно информации, чтобы действовать, чтобы защитить не только пользователя системы DNS, но и тех, кому может угрожать ее неправильное использование. Следующий слайд Сказав приятные вещи, я сейчас скажу несколько слов о болевых точках. Но помните, как я сказал, что мы должны были отправить письма о сохранении с нашими ссылками, вот почему.

65% отправленных доменов, которые я просмотрел, показывают, что владелец домена использовал услугу сохранения конфиденциальности и регистрации через доверенное лицо, обычно связанную с регистратором. Я хотел бы, чтобы вы

представили себя сотрудником службы общественной безопасности, который расследует мошенничество, фишинг и вредоносные программы с использованием тематических доменов COVID. И вы определяете несколько сотен каждую неделю. Что бы вы хотели сделать немедленно, чтобы начать работу над самым худшим из мошенников и преступников, которые этим занимаются? Я имею в виду, что вы хотели бы немедленно как можно скорее начать сравнивать данные владельцев доменов, правда? Расставить приоритеты для ваших усилий. Мы хотели сделать это. Мы просто решили, что не сможем, по крайней мере, в режиме реального времени, и это просто невозможно сделать.

В соответствии с политикой ICANN, и как в настоящее время фигурирует во временной спецификации, услуга сохранения конфиденциальности или регистрации через доверенных лиц может публиковать свои собственные правила о том, как и когда они будут отвечать на запросы общественной безопасности об информации о владельцах доменов, и стандартный для отрасли ответ был отправлен нам в судебном порядке. Когда я это говорю, я имею в виду повестку в суд или постановление суда. То, что когда-то у сотрудника службы общественной безопасности занимало 30 секунд, чтобы просмотреть данные WHOIS, где не было никакой услуги сохранения конфиденциальности или регистрации через доверенных лиц, сейчас, когда преступники в подавляющем большинстве случаев используют такие услуги сохранения конфиденциальности, для получения тех же данных в среднем требуется около 3 недель. Итак, чтобы гарантировать, что данные

будут на месте, когда мы вернемся с юридическим процессом, мы отправили письма о сохранении данных вместе со ссылками, и будут последующие раунды судебного процесса.

Наверное, много. И это будет дополнительная работа для нас. И дополнительная работа для регистраторов, и это может быть "новой нормальностью". Следующий слайд, пожалуйста. Касательно общих интернет-преступлений всех типов во время этой пандемии COVID, стоит отметить, когда мы все дома, и все больше людей работают перед компьютерами, все больше жалоб поступает в наш центр по интернет-преступности и жалобам IC3.COV. В середине графика вы увидите, что в апреле 2020 года поступило в 2 с половиной раза больше жалоб на киберпреступность, чем в апреле 2019 года. Сейчас мы в уязвимом положении, поэтому дополнительная бдительность оправдана. И я подумал, что это стоит подчеркнуть. Следующий слайд, пожалуйста. Это последний слайд по теме COVID 19.

Мы хотели сказать, что моя коллега Лорин будет представлять GAC на сквозном пленарном заседании сообщества на ICANN68, которое будет проходить сразу после этого заседания. И, говоря о Лорин, я попрошу включить ей микрофон, пожалуйста, чтобы я мог передать ей слово в отношении следующих слайдов.

LAUREEN KAPIN: Я думаю, что теперь у меня включен микрофон, мой значок микрофона указывает на это. Итак, я попрошу следующий слайд. А также спасибо всем за участие. Я знаю, что этот час не так удобен

для некоторых, как для других. Итак, последние события, связанные со злоупотреблением DNS. Некоторые очень положительные, другие немного более сложные. Во-первых, совсем недавно, всего пару дней назад, стороны, связанные договорными обязательствами, регистратуры и регистраторы приняли определение "злоупотребления DNS", и они указали, что они определяют это как состоящее из 5 широких категорий вредной деятельности, когда они пересекаются с системой доменных имен. А именно: вредоносное ПО, фишинг, фарминг и спам, когда он служит механизмом доставки для других. Например, спам, содержащий ссылку, при нажатии на которую может установиться вредоносное ПО на ваш компьютер. И это согласуется с их более ранними концепциями для борьбы со злоупотреблениями. Кроме того, Группа по анализу конкуренции, потребительского доверия и потребительского выбора также указала, что это согласуется с определением злоупотребления безопасностью DNS. И GAC, возвращаясь немного, также определил угрозы безопасности, соответствующие этому определению.

Так как было много дискуссий о том, существует ли согласованное определение злоупотребления DNS, это положительное развитие событий, что, по крайней мере, существует соглашение по основной части некоторых вредоносных действий, которые могут представлять собой злоупотребление DNS. Теперь, могут быть разные определения того, стоит ли расширять это основное определение, но это уже другая тема. Мы приветствуем это развитие событий. Другим событием, к которому это относится,

является рекомендация 14 Группы по анализу конкуренции, потребительского доверия и потребительского выбора, в которой действительно обсуждаются усилия сообщества по разработке определения злоупотребления как основа для дальнейших действий. Так что это, безусловно, очень важная часть сообщества, и мы, опять же, приветствуем эти усилия. Теперь, относительно, возможно, более сложной стороны уравнения, по-прежнему существуют проблемы с обеспечением соблюдения обязательств у отдела ICANN, и эти проблемы частично объясняются тем, что в договорах используется формулировка, определяющая правила игры для регистратур и регистраторов, и мы будем больше говорить об этом, в частности, на заседании с ALAC, посвященном обязательствам в отношении общественных интересов и проблемам, связанным с этими обязательствами, и это также позже, через пару часов. Но просто для того, чтобы дать вам общий обзор, в договорах есть требования, например, от регистратур, которые имеют нижестоящие требования для запрета злоупотребления DNS. Что я имею в виду под нижестоящими требованиями, это то, что стандартные Соглашения об администрировании домена верхнего уровня действительно говорят о том, что регистраторы должны иметь в своих контрактах положения, запрещающие владельцам доменов злоупотреблять DNS. А также сами регистратуры должны следить за злоупотреблениями DNS.

Но то, чего не хватает в контрактах, это последствий, и я скажу это очень широко. Последствий, если случится что-то плохое. Так,

например, существует обязательство по мониторингу злоупотреблений DNS со стороны регистратур, но нет конкретных указаний, что происходит дальше. И, конечно, что произойдет после того, как вы нашли злоупотребление DNS, было бы очень важно. Соответственно, регистраторы обязаны запретить своим владельцам доменов принимать участие в подобных злоупотреблениях, но эти обязательства не настолько специфичны с точки зрения того, как они должны реагировать, если владельцы доменов вовлечены в такие злоупотребления. Так что все еще есть некоторые проблемы и улучшения, которые можно внести в текст стандартных договоров. Я также хочу отметить, что с точки зрения злоупотребления DNS вы помните, я сказала сейчас, что есть некоторое хорошее согласие относительно сути того, что может представлять собой злоупотребление DNS, и, в частности, относительно этих злонамеренных действий, которые представляют собой угрозы безопасности. Но у группы по анализу доверия потребителей было более широкое определение, чтобы охватить весь диапазон злонамеренного поведения, которое может иметь место при использовании DNS, и то, что рекомендовала группа по анализу. И, признаюсь - я была частью этой группы по анализу и сосредоточила внимание на этих проблемах. Группа по анализу указала на более широкое определение, а именно то, что у вас на экране, как нечто преднамеренно обманчивое или нежелательные действия, которые активно используют DNS и / или процедуры, используемые для регистрации доменных имен.

И не включает, и это негативно, исключает, не включает в себя определенные формы контента веб-сайта ... и это относится к структуре для борьбы со злоупотреблениями, которая имела определенное исключение из этого исключения, когда контент злоупотребления является настолько вопиющим, что сторона, связанная договорным обязательством, должна действовать, когда предоставляется конкретное невероятное уведомление, так это много слов и понятий, но я думаю, что основная мысль в том, что группа по анализу, которая сосредоточилась на этих проблемах, выступает за более широкую концепцию злоупотребления DNS для выявления вредоносных действий, использующих DNS. Поэтому, хотя мы приветствуем, мы очень приветствуем тот факт, что здесь было некоторое движение, чтобы договориться, по крайней мере, о сути того, что составляет злоупотребление безопасностью DNS, мы думаем, что есть место для дальнейшего обсуждения, чтобы расширить эту концепцию. Следующий слайд, пожалуйста.

Я также хочу посмотреть вопросы в чате, и я, я думаю, что я посоветую нам прокрутить назад в конце заседания, чтобы Гейб и я могли ответить на некоторые из этих вопросов если есть время. Я просто хотела указать на это, потому что я вижу эти вопросы, и я надеюсь, что у нас будет время разобраться с ними в конце. Другие события, касающиеся злоупотребления DNS, и здесь я собираюсь сосредоточиться на некоторых других рекомендациях, сделанных группой по анализу потребительского доверия, некоторые из которых все еще находятся в статусе ожидания ... Некоторые рекомендации были приняты, некоторые были отклонены, и ряд

рекомендаций был переведен в статус ожидания. Таким образом, было предложение от группы по анализу CCT, которое было передано в PDP по последующим процедурам, о внесении предложений в отношении уменьшения злоупотреблений DNS. Но, по крайней мере, по состоянию на апрель, к сожалению, не было никакого плана, чтобы дать какие-либо рекомендации по этому вопросу. Я думаю, что есть озабоченность, что у нас есть договоры, которые применяются к новым gTLD, у нас есть договоры, которые относятся к старым gTLD, и теперь есть потенциальный второй раунд, и есть озабоченность о разных стандартах.

Я бы сказала, что если мы собираемся улучшить экосистему злоупотреблений DNS, то повышение этой планки может послужить примером для всех, к которому нужно стремиться, и в этом отношении вы можете рассматривать это как возможность, а не как негативное событие. Конечно, там есть место для обсуждения. Мы укажем на некоторые рекомендации GAC по теме рекомендаций группы по анализу доверия потребителей, которые конкретно сосредоточены на злоупотреблении DNS. И в нашем Монреальском коммюнике GAC на самом деле недвусмысленно уведомил Правление ICANN о том, что перед следующим раундом gTLD, что эти рекомендации группы по анализу потребительского доверия определяются, как предварительные условия для второго раунда или как приоритетный пункт, который должен быть реализован. И в нашем вкладе в PDP по последующим раундам, GAC выразил обеспокоенность по поводу подхода PDP по последующим раундам

и повторно заявил о необходимости выполнения рекомендаций, касающихся злоупотребления DNS, до следующего раунда.

И в настоящее время проводятся консультации по этой теме, я думаю, что темы, связанные с COVID 19 подчеркнули, что это очень важная тема, потому что, особенно во времена кризиса в области общественного здравоохранения или какого-либо другого типа кризиса, такого как стихийное бедствие, мы знаем, что это вдохновляет не только благородность людей объединяться и помогать друг другу, но и вдохновляет людей, которые хотят воспользоваться ситуацией и обществом, а также участвовать в деятельности, связанной с использованием DNS. Следующий слайд, пожалуйста. Я также хочу указать на деятельность другой важной группы по анализу безопасности и устойчивости SSR2. Они представили проект отчета в январе. Многие из их рекомендаций также были сосредоточены на усилиях по предотвращению и смягчению злоупотреблений DNS, и GAC фактически представил свой вклад по этому вопросу, публичное обсуждение одобрило многие из этих рекомендаций. Одной из конкретных вещей, которые мы поддержали, были усилия по утверждению системы DAAR, которая означает платформа отчетности о случаях злоупотребления доменами, усилия по укреплению механизмов исполнения договорных обязательств, и мы увидим окончательные рекомендации этой группы в октябре.

И еще одно, еще одно положительное событие - SSAC теперь имеет рабочую группу по вопросам злоупотребления DNS, и, конечно же, SSAC обладает особым опытом и знаниями. Мы приветствуем их

вклад и мы ожидаем, что они обсудят ... вредоносную деятельность. Есть ряд источников, называемых черными списками, они также сосредоточены на рассмотрении негативных практик, которые в настоящее время происходят в отрасли. Мы знаем, что среди определенных доменов, среди определенных ccTLD есть много инновационных практик, и они рассмотрят новые подходы и дадут рекомендации сообществу ICANN, с тем чтобы эти передовые практики стали более распространенными. И член рабочей группы по общественной безопасности был приглашен принять участие. И мое пиар-объявление здесь: во вторник, 23 июля, SSAC проведет открытое заседание, в котором вы, возможно, захотите поучаствовать. Следующий слайд, пожалуйста.

Поэтому я хочу указать коллегам GAC и всем, кто присоединяется, что будет несколько заседаний, на которых будут обсуждаться темы злоупотребления DNS, будет заседание ... для предстоящей встречей с Правлением ICANN. Во-первых, 7:00 UTC, во вторник состоится наше второе пленарное заседание GAC по злоупотреблению DNS, а затем в среду состоится наша встреча с Правлением. И некоторые из тем, которые мы ожидаем, что GAC будет рассматривать, это вопросы, связанные с услугами сохранения конфиденциальности и регистрации через доверенных лиц, и вы слышали, как мой коллега Габриэль немного об этом говорил.

Эти услуги сохранения конфиденциальности и регистрации через доверенных лиц могут усложнить задачу правоохранительных органов по выяснению того, кто стоит за вредоносной

деятельностью, связанной с определенными доменами. Мы также будем дополнительно обсуждать предупредительные меры против злоупотребления, и опять-таки они касаются рекомендаций группы по анализу доверия потребителей и, наконец, системы отчетности о точности WHOIS. Это проект ICANN, который был активным для оценки точности информация о регистрации доменных имен. К сожалению, ее деятельность была приостановлена с появлением временной спецификации и изменений, которые произошли в результате принятия закона о конфиденциальности ЕС. Но и группа по анализу CCT, и группа RDS WHOIS 2 рекомендовали возобновить этот проект, особенно потому, что он еще не достиг фазы, на которой он собирался измерить и оценить точность идентичности предоставленной информации, относящейся к владельцам доменов. И, конечно, из трех фаз, это было третьей фазой, возможно, самой важной. Поэтому есть призыв к возобновлению этого проекта. Обе эти группы по анализу. Следующие слайды, пожалуйста.

И сейчас я собираюсь сделать предварительный просмотр. Я знаю, что эта информация также была предоставлена GAC, но я собираюсь предварительно просмотреть некоторые возможные вопросы для Правления ICANN, и Гейб, я думаю, вы собираетесь ответить на этот первый вопрос, касающийся услуг сохранения конфиденциальности и регистрации через доверенных лиц.

GABRIEL ANDREWS: Мы почти закончили, ребята, но, если вернуться к понятию сохранения конфиденциальности и регистрации через доверенных лиц, потому что я ранее обозначил почему. Я просто хотел напомнить вам, почему этот вопрос существует. И мы только что обсудили, что во время этой пандемии правоохранительные органы видят огромное число преступников, на которых мы смотрим. Но в основном преступников. Всегда есть вероятность ложных позитивов или сайты скомпрометированы, но большинство из них были использованы услугами сохранения конфиденциальности и в связи с этим мы предлагали вопрос о том, что намерение Правления ICANN направлено на то, чтобы такие услуги не могли продолжать содействовать угрозам безопасности, доверию потребителей к DNS. Который в ... не может продолжать защищать злоумышленников.

LAUREEN KAPIN: Спасибо, Гейб. Иногда есть пауза, потому что есть небольшая пауза, чтобы включить нам микрофон. Переходя к вопросам о предупредительных мерах противодействия злоупотреблениям, группа по анализу CCT рекомендовала ICANN согласовать условия договора, предусматривающие финансовые стимулы для сторон, связанных договорными обязательствами, принять меры противодействия злоупотреблениям. Это было частью рекомендаций, направленных на поощрение предупредительных мер. Это находится в статусе ожидания, и были признаки того, что усилия сообщества будут направлены на разработку определения злоупотребления, поэтому нам интересно, какие шаги предприняла ICANN для содействия усилиям сообщества, у нас также есть вопрос

о том, почему существующих сообществом разработанных определений злоупотребления DNS недостаточно, и группа по анализу CCT указала на существующие определения. Последний вопрос заключается в том, рассмотрит ли ICANN вопрос о стимулировании проверки информации владельца домена регистраторами, и что я имею в виду под этим? Это означает, что система должна гарантировать, что информация, которую вы получаете о владельце домена.

Их имя. Их контактная информация, то есть фактически точная информация, и, по сути, в настоящее время есть, есть регистратуры и регистраторы, которые участвуют в этом процессе. Следующий слайд, пожалуйста, следующий вопрос касается точности регистрационных данных gTLD. Так что это также относится к нашему последнему вопросу в некотором смысле - это продолжение. Проблема недостаточной точности информации о доменном имени уже давно упоминается. И вы увидите здесь, на слайде, некоторую справочную информацию, касающуюся наблюдения первой группы проверки WHOIS, некоторую справочную информацию о системе отчетов о точности WHOIS. Опять же, группа по анализу CCT рекомендовала возобновить этот проект, чтобы перейти к последней фазе проверки личности. И это было фактически помещено в статус ожидания до результатов проверки WHOIS 2. Теперь у нас есть группа проверки WHOIS 2, рекомендующая то же самое, и эта рекомендация также находится в статусе ожидания в Правлении до группы по ускоренной

разработке политики. Полное раскрытие информации: я также являюсь частью этой команды, которая занимается этим вопросом.

И теперь мы знаем, что на самом деле на Фазе 2 команды EPDP не будет рекомендаций, касающихся системы отчетности о точности, поэтому, похоже, что возобновить этот проект не так уж далеко. Но мы знаем, что неточности данных являются постоянной проблемой. Таким образом, наш вопрос заключается в том, что Правление намеревается сделать для восстановления способности ICANN устранить неточности регистрационных данных gTLD, включая, помимо прочего, возобновление фазы проверки личности проекта системы отчетности о случаях. Следующий слайд, пожалуйста. Я думаю, что мы почти в конце. Это наше публичное объявление относительно другого заседания, которое может вас заинтересовать. Если вы присоединились к этому, вы также можете быть заинтересованы в других хороших программах, так что есть другие пленарные заседания ICANN, у нас будет пленарное заседание по злоупотреблению DNS и вредоносным регистрациям во время COVID 19 позже.

Также будет заседание, посвященное DNS и Интернету вещей, возможностям, рискам и трудностям, и, как мы все знаем, будь то наши умные термостаты или Алекса или системы в наших автомобилях, Интернет вещей в значительной степени является частью нашей жизни. Но это не только создает нам большие удобства, но и может представлять некоторые риски и проблемы, поэтому я уверена, что это будет очень интересное заседание. Заседания at large по злоупотреблению DNS и COVID 19, а также

заседание по вопросам пользователей, которое также состоится позже. А затем злоупотребление DNS: установка приемлемого порога, и это будет в среду, а затем у нас будет заседание ccNSO, посвященное ccTLD и COVID 19, так что, как вы видите, это очень горячая тема. Есть ряд заседаний, посвященных этим вопросам, и я уверена, что вы услышите множество точек зрения. С этим, я думаю, мы подходим к концу нашего заседания, и у нас есть возможность задать вопросы. Итак, отлично, я верну слово Манал, чья рука поднята, потому что мне интересно, каким будет лучший способ рассмотреть вопросы. Так что, Манал, я приветствую ваши идеи по этому вопросу.

MANAL ISMAIL, ПРЕДСЕДАТЕЛЬ GAC: Большое спасибо, Лорин и Гейб за интересную презентацию. Я пыталась отслеживать вопросы. Надеюсь, вы ничего не упустили. Итак, первый вопрос был из Непала, и вопрос следующий: можно ли объяснить злоупотребление DNS интересными бот-сетями, фишинговой фермой и спамом с помощью схематического имени или алгоритма, а не ... предложений, чтобы их было легко понять.

LAUREEN KAPIN: Я мудро передам слово Гейбу.

GABRIEL ANDREWS: Ладно. Суть в том, что вы не хотите, чтобы полицейские писали ... но, безусловно, есть графики, которые можно использовать, и,

возможно, я сделаю это в следующей презентации. У меня ничего нет под рукой, но я думаю, что особенно при обсуждении бот-сетей и т. д. Эти вещи легче визуализировать, если у вас есть картинка, и я буду использовать ее в качестве учебного материала для будущих разговоров.

MANAL ISMAIL, ПРЕДСЕДАТЕЛЬ GAC: Большое спасибо, Габриэль. Был еще один вопрос от ... и вопрос гласит: слышали ли вы какие-либо ответы относительно письма SubPro о ... о не решении проблемы злоупотребления DNS. Не кажется ли это решение опасным в свете только что представленных цифр? И хотя я надеюсь, что Кит не прочь прочитать один из своих ответов в чате, где он сказал, что Совет GNSO получил рекомендательное письмо от рабочей группы SubPro PDP и обсудит возможные последующие шаги по рекомендациям, связанным с ccTRT, связанным со злоупотреблением DNS. Мы рассматриваем ряд возможных вариантов, которые должны быть учтены целью слова, чтобы определить наиболее подходящий путь вперед. Поэтому я думаю, что могу перейти непосредственно к другому вопросу от ... вопрос к Лорин. Вы упомянули более широкий масштаб злоупотреблений DNS, процитированных в анализе CCT, и указали, что этот контент выходит за рамки этого определения. Можете ли вы помочь нам понять, где проходит граница? В качестве примера приведем несколько общих примеров злоупотребления DNS в рамках масштаба ICANN, которые выходят за рамки поведения, определенного CPH. Итак, и между скобками

определены как нарушения безопасности со стороны CCT. Итак, Лорин, могу ли я передать вам слово?

LAUREEN KAPIN: Конечно. И это справедливый вопрос, и я хотела бы, чтобы наш отчет был передо мной, потому что он, вероятно, содержит некоторые примеры. И я думаю, что я предпочитаю, чтобы Бекки рассмотрела это поближе... увидеть, что команда. Я полагаю, что это восходит к исследованию злоупотребления DNS, которое было проведено по заказу группы по анализу CCT, и которое привело некоторые очень интересные статистические данные, относящиеся к некоторым примерам системного злоупотребления DNS. Я думаю, что если бы существовали сценарии, в которых конкретные вредоносные действия и, например, обманы передавались, возможно, с помощью самого доменного имени, то это могло бы выйти за пределы основного злоупотребления безопасностью DNS, но это все еще пример использования DNS, и это то, что ICANN по-прежнему будет решать, потому что это будет эксплуатация DNS. Но я также хочу еще кое-что обсудить, но это может быть примером, который поможет. Я думаю, что мы видим, например, в контексте COVID 19, что это именно тот сценарий, в отношении которого правоохранительные органы взаимодействуют с регистраторами, где, в частности, мы рассматривали только доменные имена, потому что эти доменные имена имеют изначальное послание об обмане. Например, если есть домен, в котором написано "эффективные вакцины против COVID 19 или эффективные

лекарства против COVID 19". В настоящее время нет эффективных вакцин, и сейчас нет эффективных лекарств.

Таким образом, сообщение самого доменного имени действительно может быть проблематичным. Так что это один пример, и, вероятно, есть другие, но я надеюсь, что это полезно.

MANAL ISMAIL, ПРЕДСЕДАТЕЛЬ GAC: Большое спасибо, Лорин, и я надеюсь, что я не пропустила ни одного из вопросов, набранных в чате. Я думаю, что в чате есть довольно интересные дискуссии, и я приглашаю всех посмотреть на них. И, пожалуйста, если я пропустила ваш вопрос или комментарий, наберите его снова, и я обязательно прочитаю его вслух. Между тем - есть еще вопросы или комментарии? Хорошо, я не вижу никого. Тогда еще раз большое спасибо, Лорин и Габриэль, за эту очень интересную презентацию. Мы возвращаем всем 5 минут. Теперь снова 30-минутный перерыв. Обязательно посетите сквозное пленарное заседание сообщества по вопросам злоупотребления DNS и злоумышленным регистрациям во время COVID 19. Это запланировано на полтора часа, с 13:00 до 14:30 по времени Куала-Лумпура, с 5:00 до 6:30, а PSWG входила в состав организующей команды и Лорин участвует в группе экспертов.

За этим пленарным заседанием последует 30-минутный перерыв, затем мы соберемся здесь, в зале GAC Zoom, поэтому, пожалуйста, вернитесь в наш зал в 15:00 по времени Куала-Лумпура, 7:00 UTC, чтобы начать подготовку к нашей встрече с Правлением. Спасибо всем. Приятного отдыха.

[КОНЕЦ СТЕНОГРАММЫ]