ICANN73 | Виртуальный форум сообщества – Сессия PSWG GAC Обновление/ Злоупотребление DNS
Вторник, 8 марта 2022 г. - 14:30-15:15 ACT

GULTAN TEPE: Добро пожаловать на заседание на ICANN73 Рабочей группы GAC по обеспечению общественной безопасности по обновлению информации и злоупотреблению DNS, за которым последуют сессии GAC по обсуждению последующих раундов во вторник, 8 марта, в 18:30UTC. В целях экономии времени мы не будем проводить сегодня перекличку, но информация о присутствии членов GAC будет доступна в приложении к коммюнике и протоколе GAC.

Для обеспечения прозрачности участия в модели ICANN с участием многих заинтересованных сторон мы просим вас регистрироваться на сессиях Zoom, используя свое полное имя. Вы можете быть удалены из сессии, если не войдете в нее под своим полным именем. Если вы хотите задать вопрос или сделать комментарий, пожалуйста, напечатайте его, начав и закончив предложение словами <вопрос> или <комментарий>, чтобы все участники могли видеть ваш запрос.

Устный перевод на заседаниях GAC включает все 6 языков ООН и португальский язык. Участники могут выбрать язык, на котором они хотят говорить или слушать, нажав на значок перевода, расположенный на панели инструментов Zoom. Наконец, эта сессия, как и все другие мероприятия ICANN, регулируется Ожидаемыми

стандартами поведения ICANN. Вы можете найти ссылку в чате для ознакомления. С этим я хотела бы предоставить слово председателю GAC Манал Исмаил (Manal Ismail).

Слово предоставляется вам, Манал.

MANAL ISMAIL, ПРЕДСЕДАТЕЛЬ GAC: Большое спасибо, Гюльтен, и с возвращением всех. Я надеюсь, что вы получили удовольствие от перерыва и готовы к обсуждению проблемы злоупотребления DNS в течение 45 минут, а затем к обсуждению последующих раундов новых gTLD в течение следующих 45 минут. И у нас есть наши ведущие темы и приглашенные докладчики по смягчению последствий злоупотребления DNS. Перед нами выступят докладчики Рабочей группы GAC по общественной безопасности: Лорин Капин (Laureen Kapin), Федеральная торговая комиссия США и сопредседатель Рабочей группы GAC по общественной безопасности. Кристофер Льюис Эванс (Christopher Lewis Evans), Национальное агентство по борьбе с преступностью Великобритании, а также сопредседатель Рабочей группы GAC по общественной безопасности. Габриэль Эндрюс (Gabriel Andrews), Федеральное бюро расследований США, и наш докладчик от GAC Сумитака Ширакабе (Sumitaka Shirakabe), Япония, Министерство внутренних дел и коммуникаций и представитель GAC от Японии, а также приглашенный докладчик Иветт Пауловикс (Ivett Paulovics), соавтор исследования Европейской комиссии о злоупотреблении DNS.

Нам предстоит многое обсудить, и я думаю, что без лишних слов я передам слово нашим докладчикам, так что передаю слово нашему первому докладчику.

LAUREEN KAPIN: На этот раз это буду я. Меня зовут Лорин Капин (Laureen Kapin), и на этот раз я буду выступать в качестве сопредседателя рабочей группы GAC по общественной безопасности. Следующий слайд, пожалуйста.

Итак, вот небольшая дорожная карта того, что мы будем освещать на очень короткой, сжатой сессии. Почему смягчение последствий злоупотребления доменными именами важно, мы услышим о недавнем исследовании, проведенном по заказу Европейской комиссии о злоупотреблении DNS, и нам очень повезло, что один из авторов представит информацию об этом исследовании, так что большое спасибо.

Мы сделаем краткий обзор других последних событий, включая новую инициативу ICANN - техническую исследовательскую группу по вопросам безопасности DNS. Часть работы, проделанной SSAC, перешла в частное учреждение - Институт злоупотребления доменными именами (Domain Name Abuse Institute), который разработал новый инструмент для централизованного информирования о злоупотреблениях. Еще одна аббревиатура - CART, а также новая небольшая группа по злоупотреблениям DNS, состоящая из представителей GNSO.

Мы собираемся прорекламировать предстоящее пленарное заседание по злоупотреблениям DNS, которое будет посвящено очень важной теме различий между злонамеренно зарегистрированными доменами и взломанными доменами, и что это означает для смягчения последствий злоупотреблений DNS, мы поговорим о будущей работе, и мы услышим нашего коллегу из GAC от Японии. Мы затронем вопрос об улучшении условий контрактов и возможных оценках будущих исследований и лучших практик.

Так что давайте начнем прямо сейчас. Следующий слайд, пожалуйста. И снова мы всегда стараемся предоставить некоторую информацию о том, что это за вопросы и почему они важны, вы услышите много дискуссий/споров об определениях, но мы хотим предоставить некоторую информацию о диапазоне определений. Итак, одно из определений злоупотребления DNS и того, что под ним понимается, формулируется как угрозы безопасности, а они известны как фишинг, вредоносное ПО, ботнеты. Они взяты прямо из пекинской рекомендации GAC по механизму защиты, и эта формулировка фактически закреплена в контрактах как угрозы безопасности, которые должны отслеживаться регистратурами.

Но есть и другие определения, которые также были предложены. Группа по рассмотрению вопросов конкуренции, доверия потребителей и потребительского выбора ссылается на определение, которое было частью более раннего исследования ICANN или более раннего документа ICANN, в котором говорилось о намеренно обманных, подстрекательских или нежелательных действиях, которые активно используют DNS или процедуры,

используемые для регистрации доменных имен. И я дам ссылку на заявление GAC о злоупотреблении DNS, которое на самом деле содержит более подробное обсуждение многих различных определений и их источников.

Эти действия представляют собой угрозу для потребителей и пользователей Интернета, включая их доверие к DNS — это может быть как отдельное лицо, так и компания - или угрозу безопасности, стабильности и отказоустойчивости. Эта фраза должна звучать очень знакомо, поскольку она является неотъемлемой частью устава ICANN. Угроза безопасности, стабильности и отказоустойчивости инфраструктуры DNS. Когда мы говорим DNS, мы подразумеваем систему доменных имен.

Рабочая группа GAC по общественной безопасности была сформирована отчасти в связи с тем, что злоупотребление DNS и вопросы общественной безопасности находятся в центре внимания, и она была сформирована для того, чтобы обеспечить наличие специального канала для правоохранительных органов и защиты прав потребителей, чтобы они могли отстаивать эти вопросы, а также предоставлять консультации и поддержку Правительственному консультативному комитету по этим вопросам в качестве экспертов в данной области.

Мы были созданы в 2015 году, у нас есть план работы, техническое задание, все формальности, которые сопутствуют статусу рабочей группы Правительственного консультативного комитета.

Итак, не только GAC и Рабочая группа по общественной безопасности, но и многие группы заинтересованных сторон ICANN уделяют приоритетное внимание пресечению злоупотреблений DNS, признают и обеспокоены тем, что текущие контракты ICANN не обеспечивают достаточно четких и выполнимых обязательств по смягчению последствий злоупотреблений DNS, и есть возможности для улучшения ситуации.

Это можно найти в обсуждениях сообщества, в заявлениях отдела по обеспечению договорных обязательств ICANN, даже в переписке Правления. 12 февраля 2020 года было получено письмо от Правления ICANN, в котором говорилось о том, что, по его мнению, некоторые договорные положения не являются достаточно четкими, чтобы обеспечить выполнение обязательств. Кроме того, GAC вносил свой вклад в этот вопрос на многих различных площадках, включая обзорные группы, общественные комментарии по работе обзорных групп и участие в усилиях по разработке политики.

Такова небольшая предыстория. Кстати, эти слайды содержат очень полезные ссылки, так что, если вы хотите просмотреть их после, щелкните по ссылкам, и вы сможете самостоятельно ознакомиться с основным материалом.

Следующий слайд, пожалуйста. Итак, мы поговорим о некоторых последних событиях, первое из которых - очень подробное и информативное исследование Европейской комиссии о злоупотреблениях в системе доменных имен. Я сделаю очень краткое вступление, прежде чем передать слово моей коллеге.

Это новое исследование, проведенное по заказу Европейской комиссии. Оно вышло только в конце января, и было доведено до сведения GAC в начале февраля, а нам в Рабочей группе по общественной безопасности посчастливилось провести презентацию исследования в ходе телефонной конференции в феврале. Итак, несколько общих замечаний об этом исследовании. Оно очень практичное. Оно фокусируется на ролях и ответственности и на всей экосистеме, что очень полезно, так что оно фокусируется не только на злоупотребляющих сторонах, злоумышленниках и нарушителях, но и на посредниках, и не только на сторонах, связанных договорными обязательствами с ICANN, но даже на сторонах, даже на организациях, не сторонах, также являющихся частью этой системы.

Поэтому, когда я говорю об этом, я имею в виду, что они говорят не только о том, что могут сделать регистратуры и регистраторы. Они также говорят о том, что могут сделать хостинг-провайдеры, реселлеры и другие посредники, и это отдельно, а кроме того, к этому можно добавить правоохранительную деятельность и просвещение потребителей.

Многие рекомендации и наблюдения, которые содержатся в исследованиях, были также предложены в других проектах сообщества, например, SSAC (Консультативным комитетом по безопасности и стабильности) и другими группами проверки, включая Вторую группу по анализу и проверке безопасности,

стабильности и отказоустойчивости DNS и Группу по анализу CCT, о которой я уже упоминала.

Одна вещь, которая на самом деле очень интересна и содержательна, это их замечание о том, что очень трудно провести различие между техническими проблемами злоупотребления безопасностью, то есть фишингом, фармингом, вредоносным ПО, деятельностью ботнетов, и злоупотреблениями, связанными с контентом, потому что во многих случаях эта граница размыта из-за большого количества совпадений между различными типами злоупотреблений. И в исследовании приводится несколько примеров, но один из них говорит о фишинге, так что это может включать в себя злонамеренно зарегистрированный домен, и вы можете получить электронное письмо с этого домена, в котором говорится, что нужно перейти по этой ссылке, но затем вы можете попасть на сайты с вредоносным контентом. Таким образом, проблема злоупотребления DNS – это не только вопрос технической безопасности, но и проблема контента.

Они приводят и другие примеры, например, вредоносные программы могут использовать уязвимости в Интернете и предоставлять вредоносный контент. Одна из причин, по которой я поднимаю этот вопрос, заключается в том, что будет целая пленарная сессия, посвященная доменам, зарегистрированным со злонамеренными целями, и взломанным доменам, и это поднимает параллельные вопросы. Все для того, чтобы вы поняли сложность экосистемы, а также, что очень важно, как это соотносится с уставом ICANN и что разрешено ICANN, а что выходит за рамки ее мандата.

Следующий слайд, пожалуйста. И это последнее замечание, которое я собираюсь сделать, прежде чем вы услышите непосредственно автора исследования. Некоторые выводы, некоторые фактические выводы, которые представляют интерес, я думаю, особенно для GAC, заключаются в том, что новые gTLD являются одной из наиболее злоупотребляемых групп gTLD в относительном выражении. Так, если вы посмотрите на первый график, то увидите стрелку, указывающую на чуть более 6%. Это процент рынка, на котором присутствуют новые gTLD, так что из всех gTLD новые gTLD составляют около 6%.

Если посмотреть на злоупотребляемые домены, то можно увидеть, что процент злоупотреблений доменными именами в новых gTLD гораздо выше по сравнению с 6%. Он составляет более 20%. Так что это интересный факт, который следует учитывать, особенно когда мы рассматриваем новые раунды gTLD.

Они также отмечают, что на два наиболее злоупотребляемых новых gTLD приходится около 41% всех злоупотреблений именами. Это концентрация. Это не все новые gTLD. Злоупотребления DNS сосредоточены в нескольких новых gTLD. Они также приводят наблюдения о злоупотреблениях на уровне регистраторов, отмечая, что и здесь наблюдается определенная концентрация. На пятерку наиболее подверженных злоупотреблениям регистраторов приходится 48% всех злонамеренно зарегистрированных доменных имен, и они также отмечают, что регистраторы и поставщики услуг, подвергающиеся злоупотреблениям, могут очень быстро

реагировать на сообщения о злоупотреблениях и принимать быстрые и решительные меры, которые могут уменьшить воздействие и вред.

Таким образом, правоохранительные органы, службы защиты прав потребителей и правительственные организации призывают людей сообщать о злоупотреблениях, потому что во многих случаях регистраторы и поставщики услуг относятся к этому очень серьезно, что только на пользу. И с этим я хотела бы передать слово автору исследования Европейской комиссии, Иветт, пожалуйста, вам слово и заранее спасибо за то, что согласились прийти сюда сегодня и позволить нам глубже погрузиться в это очень важное исследование.

IVETT PAULOVICS: Большое спасибо, Лорин, и спасибо, что пригласили меня сюда. Из-за нехватки времени я сразу перейду к своей презентации. Итак, я расскажу о целях исследования, которое было поручено нам Европейской комиссией, методологии, которую мы использовали, сроках, определении, которое мы предложили для злоупотребления DNS, величине, которую мы измеряем, передовом опыте, который мы выявили, и рекомендациях. Следующий слайд, пожалуйста.

Итак, цель этого исследования была довольно широкой, поэтому нам было поручено оценить феномен злоупотребления DNS, найти определение, выявить повторяющиеся случаи, типологии. Оценить роль действующих лиц, а также оценить масштабы этого явления. Дать обзор политики и законов на международном уровне, уровне ЕС, ICANN, а также определить отраслевую практику и, по

возможности, определить передовую практику, которую можно распространить на других посредников или на уровне ЕС, международном уровне и ICANN, а также определить технические и политические меры, необходимые для решения проблемы злоупотребления DNS.

Следующий слайд, пожалуйста. Методология, которую мы использовали, состояла из одной части первичного исследования, то есть мы проводили измерения в реальном времени, опросы, подробные интервью, а также организовывали семинары. В ходе измерений в режиме реального времени мы проанализировали более 2,7 млн. инцидентов и 1,68 млн. неправомерно используемых доменных имен, используя черный список, черный список доменов и URL, а что касается вторичных исследований, мы провели довольно обширный обзор отчетов третьих сторон.

Следующий слайд, пожалуйста. Это исследование заняло один год, и мы проводили измерения во втором квартале 2021 года, то есть с марта по июнь.

Следующий слайд, пожалуйста. Что касается определения злоупотребления DNS, Лорин уже упомянула об ограничении многих терминологий, которые использовались до сих пор. Мы обнаружили, что довольно сложно провести различие между техническими угрозами и угрозами, связанными с контентом, из-за широкого дублирования этих типов угроз, поэтому мы предлагаем использовать более широкое определение: злоупотребление системой доменных имен — это любая деятельность, которая

использует доменные имена или протокол DNS для осуществления вредоносной или незаконной деятельности.

Наш подход основан на принципе «снизу вверх» для анализа каждого случая, и самое главное, что следует отметить, что наш подход проводит различие между доменными именами, зарегистрированными со злонамеренными целями, и взломанными доменными именами, то есть теми доменными именами, которые были зарегистрированы законными владельцами доменов, но на более поздней стадии были взломаны злоумышленниками из-за уязвимости веб-хостинга или по другим причинам.

Следующий слайд, пожалуйста. Как мы классифицируем злоупотребления DNS? В исследовании мы выделяем 3 категории. Тип 1 включает в себя злоупотребления, связанные с регистрацией доменных имен со злонамеренными целями. Тип 2 - злоупотребления, связанные с работой DNS и других инфраструктур. И тип 3 - злоупотребления, связанные с доменными именами, распространяющими вредоносный контент. Важно подчеркнуть, что этот третий тип может воспользоваться доменными именами, зарегистрированными со злонамеренными целями, или взломанными доменными именами.

Следующий слайд, пожалуйста. Этот подход также важен, и различие между доменными именами, зарегистрированными со злонамеренными целями, и взломанными доменными именами позволяет прийти к вопросу и ответу о том, кто должен принять меры для смягчения последствий злоупотребления DNS.

Первая категория: злоупотребления, связанные с доменными именами, зарегистрированными со злонамеренными целями. Например, алгоритмически генерируемые домены, используемые для командно-контрольной связи. По нашему мнению, путь к устранению должен быть на уровне DNS, поэтому посредники, которые должны принимать меры, находятся на этом уровне, уровне DNS.

Что касается вредоносного контента, как мы уже говорили, он может распространяться с использованием доменных имен, зарегистрированных со злонамеренными целями, например, доменных имен с опечатками, обслуживающих фишинговый контент. В этом случае путь к устранению должен проходить на уровне хостинга, а также на уровне DNS. Это связано с тем, что защита от такого рода злоупотреблений только на одном уровне будет неэффективной.

В случае распространения вредоносного контента с использованием взломанных доменных имен, например, взломанного домена, обслуживающего фишинговый контент, нецелесообразно устранять такие злоупотребления на уровне DNS, поскольку это может нанести побочный ущерб законному владельцу домена, а также пользователям, поэтому в этом случае мы предлагаем устранить проблему на уровне хостинга.

Что касается злоупотреблений, связанных с работой DNS, то они должны решаться на уровне DNS. Таким образом, из предложенного

нами определения следует, кто должен принимать меры по борьбе со злоупотреблениями DNS.

Следующий слайд, пожалуйста. Давайте теперь поговорим о масштабах злоупотребления доменами. Лорин уже упомянула об одном из графиков исследования. Мы измерили общее состояние TLDs, мы также измерили, где происходит злоупотребление, то есть доменные имена, зарегистрированные со злонамеренными целями, и взломанные доменные имена. Репутация регистратора. Репутация хостинг-провайдера, а также другие вопросы, такие как время безотказной работы. Что касается общего состояния TLDs, как упомянула Лорин, мы пришли к выводу, что на этом графике вы можете видеть, на этом рисунке вы можете видеть, потому что он сравнивает долю рынка пяти групп TLDs с распределением доменов из черного списка, и мы пришли к выводу, что EU ccTLDs являются наименее подверженными злоупотреблениям как в абсолютном выражении, так и относительно их доли рынка. Вы можете видеть, что, например, EU ccTLDs имеют 14,44% доли рынка и менее 1% злоупотреблений.

В относительном выражении новые gTLD, как уже упоминалось Лорин, с долей рынка в 6,6%, являются наиболее подверженной злоупотреблениям группой gTLD, Лорин также отметила, что результаты исследования не означают, что все новые gTLD подвергаются злоупотреблениям, поскольку мы заметили, что два наиболее подверженных злоупотреблениям новых gTLD вместе взятые составляют 41% от всех подверженных злоупотреблениям новых gTLDs.

Следующий слайд, пожалуйста. На следующем рисунке показано распределение взломанных доменных имен и доменных имен, зарегистрированных со злонамеренными целями, по типам злоупотреблений. Здесь мы видим, что около 25% и 41% фишинговых и вредоносных доменов предположительно взламываются на уровне хостинга. В то время как подавляющее большинство спама и командно-контрольных доменов ботнетов зарегистрированы злонамеренно.

Следующий слайд, пожалуйста. На этом рисунке показано распределение взломанных и злонамеренно зарегистрированных доменов по типам TLD. Следующий слайд, пожалуйста. Затем, как я уже говорила, мы измеряем эти показатели через репутацию. Репутация хостинг-провайдера, и мы заметили, что на пять наиболее подверженных злоупотреблению регистраторов приходится 48% всех злонамеренно зарегистрированных доменных имен. Мы также отметили непропорционально высокую концентрацию спамовых доменных имен среди хостинг-провайдеров.

Мы также заметили, что общий уровень расширений безопасности DNS и протоколов защиты электронной почты, таких как DMARC и SPF, остается очень низким. Следующий слайд, пожалуйста. Наконец, после анализа всех политик, применяемых на международном уровне, уровне ЕС, уровне ICANN, а также некоторых саморегулируемых организаций, мы определили передовые практики различных типов, поэтому мы разделили такие передовые практики на превентивные, реактивные передовые

практики, а также в отношении прозрачности и доступности информации, и затем мы определили различных посредников, поэтому вы можете видеть примеры ccTLDs, а также некоторых регистратур gTLD.

Из-за нехватки времени я не могу подробно рассказать о передовой практике, так как в исследовании она подробно проанализирована, поэтому я перейду к следующему слайду.

И, наконец, в исследовании мы определили набор из 27 рекомендаций в шести различных областях, чтобы улучшить меры по смягчению последствий злоупотреблений DNS. Здесь я, конечно, не могу упомянуть все рекомендации. Есть некоторые технические, а также некоторые рекомендации, связанные с политикой. Так, например, эти рекомендации касаются различных посредников. Так, например, для регистратур, регистраторов и реселлеров мы рекомендовали создать стандартизированную или централизованную систему регистрации злоупотреблений для проверки точности данных регистрации доменных имен с помощью процедур «знай своего клиента», использовать алгоритмы прогнозирования для мониторинга уровня злоупотреблений, а также использовать санкции и стимулы для того, чтобы удержать уровень злоупотреблений ниже установленных пороговых значений.

В отношении хостинг-провайдеров мы также определили аналогичные рекомендации по мониторингу уровня злоупотреблений, который не должен превышать установленные пороговые значения. И в рамках, скажем так, последней области

сотрудничества, повышения осведомленности и накопления знаний на уровне ЕС мы рекомендовали гармонизировать работу ccTLD путем принятия передовой практики, которая была выявлена, а также сотрудничать с правительственными учреждениями, правоохранительными органами и доверенными нотификаторами, так что есть несколько рекомендаций, которые, как упомянула Лорин, могут также наблюдаться в различных других исследованиях, но это исследование попыталось дать полный обзор явления, что мы наблюдали в 2021 году.

Это был мой последний слайд, и, возможно, на последнем слайде вы найдете ссылки на скачивание исследования, а также вы можете связаться со мной или с моим соавтором Мацеем Корчински (Maciej Korczynski) из Гренобльского университета, который не может присутствовать на этой сессии, потому что он одновременно выступает на Бизнес-конференции, поэтому большое спасибо за предоставленное время.

LAUREEN KAPIN: Большое спасибо, и я знаю, что Манал предложила, и я уже вижу вопросы в чате и поднятые руки, сделать небольшую паузу для тех, у кого могут быть вопросы конкретно по исследованию, я также отмечу, что нам нужно многое успеть до окончания работы, 2:15, и прошу всех помнить об этом.

Финн спросил, есть ли какие-нибудь легкие решения, есть ли что-нибудь в плане рекомендаций, что было бы особенно легко выполнить как можно скорее? И я думаю, что этот вопрос адресован вам, Иветт.

IVETT PAULOVICS: Да. Спасибо, извините, у меня был выключен звук. Итак, это, очевидно, непростой вопрос и он зависит от …. это исследование было заказано Европейской комиссией, так что для Европейской комиссии, например, может быть гораздо проще обратиться к ccTLDs в ЕС, чтобы гармонизировать работу ccTLD, перенимая передовой опыт. В рамках ICANN, возможно, есть другие приоритеты и другие рекомендации, которые было бы легче принять, также потому, что существует много других параллельных проектов.

LAUREEN KAPIN: Сьюзан, полагаю, вы следующая.

США: Спасибо, Лорин. Мы искренне признательны за исследование по злоупотреблению DNS, которое представляется всеобъемлющим ресурсом для разработчиков политики, стремящихся лучше понять технические и коммерческие слои, на которых происходит как незаконная, так и законная деятельность в Интернете.

Но в то же время, кажется, что определение злоупотребления DNS в этом исследовании может быть слишком широким для использования в рамках ICANN, поскольку это определение может охватывать вредоносную и незаконную деятельность в Интернете, которая не входит в полномочия ICANN по уставу, но с учетом сказанного, мы считаем, что это место идеально подходит для содействия обмену мнениями между правительственными

экспертами по вопросам политики DNS, в том числе по исследованию комиссии.

Даже если некоторые из этих вопросов выходят за рамки устава ICANN, я думаю, что в целом, мы ценим исследование, мы признаем его полезность, и мы также признаем, что по широкому определению злоупотребления DNS могут рассматриваться в рамках ICANN, но также и за пределами ICANN, поэтому большое спасибо.

LAUREEN KAPIN: Спасибо. Хемма, вы следующая.

GEMMA CAROLILLO: Я надеюсь, что вы меня хорошо слышите, потому что у меня были небольшие проблемы со звуком. Я также вижу себя, поэтому, прежде всего, большое спасибо Иветт за презентацию, а также Мацею, который действительно параллельно участвует в других сессиях, и это по двум причинам. Во-первых, потому что наши подрядчики, конечно, были очень полезны и очень помогают в распространении информации о проделанной ими работе, а также потому, что с нашей стороны было немного подталкивания к тому, чтобы они действительно вели диалог с сообществом ICANN на многих форумах, насколько это было возможно.

Так что спасибо, Иветт, за вашу презентацию, и, как упомянула в начале Лорин, от PSWG также была довольно обширная презентация. Я была удивлена и положительно удивлена резюме, которое Лорин сделала в начале, потому что действительно есть вещи, которые обсуждались в PSWG, которые, возможно, могут быть

рассмотрены, и это частично отвечает на вопрос Финна о легких решениях, рассматривая то, что, возможно, может быть предложено в контексте контрактов ICANN в отношении злоупотребления DNS, потому что это тема, которая обсуждалась в ICANN.

Это было предметом обсуждения после выпуска отчетов SSR2, и это то, над чем также работает группа PSWG в плане возможных предложений.

Я хочу сказать пару вещей. Во-первых, наш подход заключается в том, что наше исследование является независимым, поэтому мы поручили его экспертам, не входящим в состав Комиссии. Мы заказали это исследование даже, я бы сказала, без конкретного графика для инициативы по политике, что обычно имеет место в Европейской комиссии, просто потому, что эта тема очень важна для нас, и необходимость предотвращения и поиска злоупотреблений DNS занимает центральное место в главе о безопасности и открытости Интернета в Европейской стратегии кибербезопасности 2020 года.

Наше намерение предоставить максимально широкую видимость и время для обсуждения в ICANN для этого исследования связано с тем, что ICANN приравнивается к DNS за использование упрощенного подхода, и мы постоянно напоминаем, что ICANN является местом, где DNS необходимо обсуждать и где необходимо принимать меры. Поэтому мы хотим, чтобы исследование было очень заметным в повестке дня ICANN, и, конечно, очень важно, чтобы различные

группы имели возможность прокомментировать его, потому что, конечно, это независимое исследование. Это не Библия.

И поэтому есть элементы, которые могут потребовать пересмотра или комментарии, которые могут быть высказаны с учетом различных интересов, но это ни в коем случае не исследование ICANN. Поэтому я хотела бы, я надеюсь, и вот уже второй или третий раз представляется это исследование, что мы немного прекратим риторику о том, что может сделать ICANN. Это не входит в компетенцию ICANN.

То есть, я думаю, что все в сообществе заинтересованы в предотвращении и борьбе со злоупотреблениями DNS. Злоупотребление DNS — это очень сложная тема, потому что, конечно, как очень хорошо представила Иветт, это не начинается и не заканчивается регистрацией доменных имен со злонамеренными целями. Это может произойти после регистрации доменного имени. Это может произойти на более поздней стадии, и в этом могут участвовать несколько субъектов. Я думаю, что огромные усилия, которые подрядчики приложили именно для того, чтобы рассмотреть злоупотребление DNS комплексно, должны быть, знаете ли, я думаю, именно главной дополнительной ценностью.

Мы рассматриваем злоупотребление DNS со стороны тех, кто от него страдает. Поэтому, возможно, строгое определение и, я бы сказала, споры о том, что именно является злоупотреблением DNS, могут быть прекращены или, по крайней мере, я имею в виду, приостановлены, чтобы увидеть, что происходит под зонтиком

злоупотребления DNS, происходит через использование DNS или путем регистрации доменных имен со злонамеренными целями, и вот какие субъекты вовлечены.

Мы можем видеть это очень четко, и исследование, которое, конечно, очень длинное и не все детали могут быть представлены в этом контексте, четко рассматривает, что могут сделать регистратуры, регистраторы, реселлеры, потому что я видела, конечно, есть очень сложная среда после регистраторов, но это точно определено в исследовании, и что могут сделать хостинг-провайдеры.

И в некоторых случаях в исследовании выделяются злоупотребления DNS типа 1, 2 и 3 в зависимости от того, на каком уровне это происходит, злоупотребление. Необходимо участие более чем одного субъекта, поэтому первый шаг заключается в том, чтобы субъекты действительно имели возможность информировать друг друга о том, что что-то происходит. Вот почему одно из легких решений - пожалуйста, имейте контакты, по которым можно сообщить о злоупотреблениях. Это была одна очень, очень четкая и небольшая рекомендация, которая может изменить ситуацию.

Убедитесь, что кто-то несет ответственность внутри организации за обработку таких запросов, и убедитесь, что участники, которые хотят общаться на уровне хостинга или на уровне DNS, имеют возможность связаться с ответственными лицами. И, конечно, это также четко указывает на необходимость наличия хороших записей WHOIS. Это еще один четкий вывод из исследования.

Итак, конечно, я хочу сказать, что это очень длинная тема, и я не хочу заменять презентацию Иветт, но я действительно хотела сказать, что я думаю, что люди в ICANN, в сообществе ICANN возьмут из исследования то, что вы считаете полезным. Есть много рекомендаций, адресованных операторам, мы, как Европейская комиссия, можем посмотреть, что мы, как разработчики политики, можем сделать, и это то, что мы делаем с нашей стороны. Мы оцениваем рекомендации с этой точки зрения.

Но нам бы очень хотелось, чтобы сообщество оценило ситуацию. Если есть что-то, что представляется ценным, и в сроки, которые мы видим, мы заново оценим, что произошло, если что-то произошло, и были ли сделаны улучшения. Но мне бы очень хотелось сказать: давайте посмотрим, что можно сделать, вместо того чтобы сосредотачиваться на узких или широких полномочиях ICANN. Дело не в этом. Мы не просим рассматривать только ICANN. Это часть экосистемы. Спасибо, Лорин. Извините за очень длинное выступление, но я подумала, что должна прояснить несколько моментов.

LAUREEN KAPIN: Спасибо, Хемма. Я надеюсь, Манал, что мы сможем уделить еще несколько дополнительных минут, поскольку вопросы и утверждения исследования были очень полезны, и, естественно, когда что-то полезно, это занимает больше времени. Но прежде всего вам не нужно отвечать на этот вопрос сейчас. Мы вернемся к слайдам и изменим порядок, так что, если я могу спросить, отлично.

Если мы можем сразу перейти к моей коллеге из Японии, потому что мы хотим быть уверены, что мы дойдем до этого материала, а затем, возможно, мы сможем оценить, сможем ли мы сделать очень быстрый обзор оставшегося материала. Так что моей коллеге из Японии большое спасибо за терпение.

SUMITAKA SHIRAKABE: Большое спасибо. Говорит Ширакабе, вы меня слышите?

LAUREEN KAPIN: Да.

SUMITAKA SHIRAKABE: Хорошо, большое спасибо. Спасибо, Лорин. Я очень признательна за эту возможность, а также знаю, что у нас осталось довольно мало времени. Поэтому сегодня я быстро представлю вам этот слайд, всего один слайд.

Итак, сегодня, пользуясь возможностью, я хотела бы поделиться этим слайдом. Во время последнего заседания GAC на ICANN72 мы обсуждали вопрос о так называемом «перепрыгивании между регистраторами». Владелец домена злоупотребляет, перенося одни и те же доменные имена от одного регистратора к другому регистратору. Сегодня это новая и актуальная проблема. Мы хотели бы поделиться случаем, когда владелец домена, который казался одним и тем же, продолжает злоупотреблять, используя различные доменные имена, зарегистрированные у одного и того же регистратора.

Таким образом, это актуальная проблема. Наша точка зрения, с японской стороны. И сегодня мы хотели бы предложить вам два момента. Первый пункт — это обеспечение соответствия между ICANN, регистратурой и регистратором.

Конечно, многие коллеги уже упоминали об этом. Я знаю, что по-прежнему важно корректировать информацию от владельца домена во время регистрации домена и обеспечивать точность информации, а также очень важно проводить эффективный и постоянный аудит соответствия регистратора договорным требованиям ICANN.

Второй момент — это рассмотрение эффективных мер против злоупотреблений при использовании доменных имен. Одна из идей, которую мы рассматриваем, касается возможности использования так называемой программы доверенных нотификаторов. Я думаю, что это было бы полезно, особенно в случае злоупотребления DNS, которое содержит вопрос контента. Кроме того, я бы предложила совместную работу, обсуждение с другими организациями поддержки или консультативными комитетами ICANN.

Насколько я помню, на последнем заседании GAC на ICANN72, ICANN72 с ALAC, обсуждался вопрос о продвижении дискуссии относительно злоупотребления DNS между GAC и ALAC и упоминалось о создании малой группы.

Это было бы хорошей идеей, и мы действительно ожидаем таких действий. Кроме того, сегодня утром было упомянуто о группах

ccNSO, и мы действительно ожидаем такого инициативного подхода и действий в нескольких группах, а также ожидаем совместной работы между GAC и другими группами.

Итак, как многие коллеги уже упомянули, есть некоторые организации, есть что-то ограниченное в ICANN, но мы действительно ожидаем, что ICANN предпримет больше действий, предупреждающего характера в отношении проблемы злоупотреблений. Вот и все на сегодня. Большое спасибо, Лорин, за предоставленную возможность. Спасибо.

LAUREEN KAPIN: Большое спасибо, Сумитака. Мы высоко ценим вашу презентацию.

MANAL ISMAIL, ПРЕДСЕДАТЕЛЬ GAC: Итак.

LAUREEN KAPIN: Продолжайте, пожалуйста.

MANAL ISMAIL, ПРЕДСЕДАТЕЛЬ GAC: Лорин, это говорит Манал. Извините, что прерываю вас, и большое спасибо Сумитаке. Я использую мои резервные каналы, мы заняли десять минут у Луизы и Хорхе, так что у вас есть время до 25 минут, пожалуйста. Переходим к вам.

LAUREEN KAPIN: Хорошо. Отлично. Итак, Гейб, я передаю эстафету вам, но могу я попросить сотрудников ICANN вернуться на несколько слайдов назад. Продолжайте. Продолжайте, продолжайте. Хорошо, еще один слайд вниз.

GABRIEL ANDREWS: Четвертый.

LAUREN KAPIN: Вот так. Итак, Гейб, ваша миссия, если вы решите ее принять, будет заключаться в том, чтобы дать очень краткий обзор оставшегося материала, пока я не возьму слово в самом конце. Вперед!

GABRIEL ANDREWS: Мы сделаем это быстро, друзья. Отличная презентация исследования ЕС, несмотря на то, что это было не единственное важное исследование, опубликовавшее результаты в последнее время, и я хотел бы воспользоваться моментом, чтобы подчеркнуть отличную работу, которая была проделана в рамках так называемых инициатив по содействию безопасности DNS и их технической исследовательской группы. Для справки, это то, что генеральный директор ICANN запросил еще в 2020 году, и это было ответом на некоторые очень громкие атаки, направленные на инфраструктуру DNS. 2018, 2019 годы, такие атаки, как Sea Turtle и DNSpionage, которые вы могли видеть в новостях. TSG, Техническая исследовательская группа, изучила не только эти атаки, но и многие другие реальные атаки и опубликовала примеры, взятые из этих реальных инцидентов, а также лучшие общие практики для решения этих реальных инцидентов безопасности.

Поэтому, не слишком углубляясь в эту тему, все рекомендации будут направлены в офис главного технического директора ICANN, который был одним из авторов отчета. Возможно, в результате этой работы ICANN позже подготовит дополнительные комментарии, но немедленной необходимости в действиях GAC нет. Я просто хочу подчеркнуть превосходную работу, проведенную здесь.

Следующий слайд, пожалуйста. Возможно, вы помните, что примерно в прошлом году Консультативный комитет по безопасности и стабильности, SSAC, опубликовал свой SAC 115, отчет о решении проблемы злоупотреблений и о том, как с этим бороться. В нем была одна рекомендация, и эта рекомендация касалась создания общего координатора по реагированию на злоупотребления.

С тех пор, год спустя, мы начинаем видеть, как может выглядеть один из возможных кандидатов на роль такого координатора реагирования на злоупотребления, и мы видим его в лице Института злоупотреблений DNS, который был создан Реестром общественных интересов. Сейчас они тестируют нечто под названием «Централизованный инструмент отчетности о злоупотреблениях». Я не думаю, что это официальное название, сейчас мы называем его CART. Он может быть запущен уже в июне. Его цель - автоматизировать маршрутизацию жалоб на злоупотребления. Возможно, даже обогатить их дополнительной отчетностью, которая облегчит договорным сторонам получение и обработку этой отчетности. Так что это очень предварительная информация. Но это

нечто новое и интересное, и мы надеемся, что, возможно, на следующей конференции ICANN мы сможем углубиться в изучение этого инструмента.

Следующий слайд. Верно. Завершая обзор других событий, отметим, что Организация поддержки доменов общего пользования (GNSO) недавно создала небольшую группу по злоупотреблениям DNS. И в рамках своей работы они начали обмениваться вопросами, включая вопросы, представленные в GAC, чтобы лучше понять, что ожидается от GNSO, и может ли дальнейшая работа по политике способствовать их существующим инициативам.

Эти вопросы представлены здесь на слайде. Я не буду сейчас углубляться в них, но имейте в виду, что эти вопросы были заданы, и малая группа по злоупотреблению DNS в GNSO, возможно, амбициозно, ожидает ответа к 21 марта. Если кто-то хочет внести свой вклад, пожалуйста, подключайтесь.

Следующий слайд. Наконец, совсем скоро, завтра, состоится пленарное заседание, посвященное доменам, зарегистрированных со злонамеренными целями, и взломанным доменам. Мы отмечаем, что в исследовании Европейской комиссии говорилось о том, что могут существовать различные пути эскалации для направления сообщений о злоупотреблениях в зависимости от их характера. Эта дискуссия будет посвящена именно этому вопросу, и я думаю, что она будет интересной.

И с этим я передаю бразды правления вам, Лорин.

LAUREEN KAPIN: Спасибо. Следующий слайд, который, я думаю, является последним. Мы уже выслушали нашего коллегу. Это слайд о будущей работе, но в последнюю минуту просто подчеркну одну из вещей, над которой мы по-прежнему хотим работать, - это улучшение требований к контрактам, и у нас действительно были некоторые формулировки в нашем последнем коммюнике, которые указывали на положения во внутренних документах, которые уполномочивали ICANN вести переговоры по договорам, включающим обязательства по обеспечению общественного интереса для выполнения своей миссии. Поэтому мы считаем, что работа может быть проведена совместно с заинтересованными сторонами и ICANN для достижения этих целей по улучшению положений договора, чтобы еще больше реагировать на злоупотребления DNS, а также что необходимо провести дальнейшую оценку злоупотреблений DNS.

В частности, наш Консультативный комитет по безопасности и стабильности рекомендовал провести определенную работу, особенно перед запуском следующего раунда новых gTLD, что, на мой взгляд, является отличным переходом к нашей следующей сессии, поскольку при рассмотрении дополнительного раунда новых gTLD, конечно, всегда полезно изучить уроки, извлеченные из злоупотреблений DNS в последнем раунде и в целом.

Итак, я хочу извиниться, что у нас не было больше времени для вопросов, которые у вас могли бы возникнуть, но я, конечно, приглашаю вас обращаться в Рабочую группу по общественной

безопасности в любое время, не только во время этих встреч, если у вас есть вопросы, мы будем рады побеседовать с вами. Итак, с этим я передаю вам слово, и думаю, что я успела как раз вовремя, поскольку у меня было дополнительное время.

MANAL ISMAIL, ПРЕДСЕДАТЕЛЬ GAC: Спасибо. Большое спасибо, Лорин, Крис, Габриэль, Сумитака и Иветт, очень интересно и познавательно, и я хочу поблагодарить Фабьена за поддержку, которую он оказывает PSWG. И без дальнейших задержек я передаю слово нашим ведущим тем по последующим процедурам.

[КОНЕЦ СТЕНОГРАММЫ]