ICANN83 | Форум по вопросам политики – Обсуждение GAC вопросов борьбы со злоупотреблениями DNS
Вторник, 10 июня 2025 г. – с 09:00 до 10:15 CEST

JULIA CHARVOLEN: Приветствуем вас на заседании GAC в рамках ICANN-83, посвященном борьбе со злоупотреблениями DNS, которое состоится во вторник, 10 июня, в 7:00 по Гринвичу. Обращаем ваше внимание, что это заседание записывается и проводится в соответствии с Ожидаемыми стандартами поведения ICANN и Политикой ICANN по борьбе с домогательствами. Во время этого заседания вопросы или комментарии будут зачитываться вслух только в том случае, если они будут представлены в надлежащей форме в чате Zoom. Устный перевод на этом заседании будет осуществляться на все шесть языков ООН и португальский язык. Если вы хотите выступить на этом заседании, пожалуйста, поднимите руку в зале Zoom. Когда вам будет предоставлено слово, вы сможете включить звук в Zoom. Пожалуйста, для протокола назовите свое имя и язык, на котором будете говорить, если это не английский, и говорите в разумном темпе, чтобы обеспечить точность перевода. Сейчас я передаю слово председателю GAC Нико Кабальеро (Nico Caballero). Спасибо, слово вам.

NICO CABALLERO: Спасибо, Джулия. Приветствую всех, а также приветствую ведущих по темам и приглашенных докладчиков: Мартина

Кунца (Martin Kunc) из Национальной CSIRT Чешской Республики, Карин Роуз (Karin Rose) и Грега Аарона (Greg Aaron) из компании Interisle Consulting Group, Грэма Бантона (Graeme Bunton) из Института NetBeacon, Сьюзан Чалмерс (Susan Chalmers), которую вы, конечно, уже знаете, она представитель США и ведущая по темам PSWG, у нас есть Янош Дриеньовски (Janos Drienyovszki) из Европейской комиссии и г-н Миямото Томо (Miyamoto Tomo) из Японии.

Приветствую всех. Нас ждут очень интересные дискуссии по борьбе со злоупотреблениями DNS, а затем, я надеюсь, мы перейдем к интересной и увлекательной сессии вопросов и ответов. Так что, без лишних слов, передаю слово Томо. Вам слово.

TOMONORI MIYAMOTO

Спасибо, председатель. Доброе утро всем, добрый день и добрый вечер коллегам, присоединившимся к нам онлайн. Томонори Миямото (Tomonori Miyamoto) из Японии, и я надеюсь на плодотворную дискуссию сегодня. Вот повестка дня этого заседания. После краткого представления я расскажу о последних событиях в области злоупотреблений DNS и мерах по борьбе с ними, уделив особое внимание фишингу. В качестве доклада принимающей страны CZ NIC представит свою кампанию по борьбе с фишингом, а затем все участники поделятся своими мнениями.

Во второй части мы обсудим PDP, процесс разработки политики для следующего этапа. Мы сосредоточимся на PDP с узкой направленностью, чтобы сократить сроки, учитывая делегирование новых gTLD в следующем году. Следующий слайд, пожалуйста. Вот некоторые сведения о злоупотреблениях DNS. Договоры ICANN RA и RAA требуют от регистратур gTLD и регистраторов принимать меры по борьбе со злоупотреблениями DNS, когда они получают сообщения о злоупотреблениях DNS, требующие принятия мер.

Существуют различные понимания и контексты злоупотребления, возможно, включая фишинг, мошенничество, нарушение авторских прав, например, в моей стране, Японии, большую проблему представляет пиратство манги. Однако определение злоупотребления DNS в договоре ICANN ограничено и включает распространение вредоносного ПО, ботнеты, фишинг, фарминг и спам. Поправка к этому договору, внесенная в 2024 году, является первым шагом на пути к борьбе со злоупотреблениями DNS, и мы рассматриваем и принимаем дальнейшие меры для решения проблемы злоупотреблений DNS.

Следующий слайд, пожалуйста. Спасибо. Некоторые из вас, возможно, знакомы с этой диаграммой. Она показывает всю экосистему или ландшафт этого вопроса. Ограничение или сфера действия договора ICANN обозначена зеленым квадратом слева, и она довольно ограничена. Для эффективного решения проблемы нам, возможно,

необходимо рассмотреть отношения, обозначенные синим квадратом, такие как договор между регистраторами и реселлерами.

Мы также можем рассмотреть сотрудничество между расширенным сообществом в рамке красного квадрата, например, программу доверенного уведомителя. Сегодня мы сосредоточимся на зеленом квадрате, где указаны возможные PDP, с учетом следующего раунда новых gTLD в следующем году. Однако мы должны учитывать всю картину, связанную с договором. Следующий слайд, пожалуйста. На предыдущей конференции ICANN в Сиэтле мы рассмотрели ситуацию и доказательства по борьбе со злоупотреблениями, включая отчет INFERMAL.

На прошлой неделе мы провели вебинар GAC перед ICANN-83, на котором Институт NetBeacon представил возможные идеи по PDP, а стороны, связанные договорными обязательствами, поделились своими взглядами и ответами. Кроме того, в апреле этого года начала работу малая группа GNSO по злоупотреблениям DNS, которая представила свои сроки и цели. Сотрудничество с этой малой группой по злоупотреблениям DNS должно стать нашим возможным дальнейшим шагом.

И сегодня, в ходе этой дискуссии, мы обсудим разработку политики. Следующий слайд, пожалуйста. Это последний слайд вводной части. Он не является на 100% точным, но я

визуализировал и систематизировал некоторые темы и дискуссии по злоупотреблениям DNS. Вы можете видеть двустороннюю стрелку на правой Меры, принимаемые во время сообщения о злоупотреблении и его устранения, можно назвать реактивными мерами или мерами по борьбе со злоупотреблениями. Здесь приведены обязательства, основанные на договоре с ICANN, о которых я уже говорил, и мы могли бы подумать о сообщении информации для обеспечения транспарентности в дополнение к отличной работе группы ICANN по обеспечению выполнения договорных обязательств.

Мы также можем рассмотреть меры по сокращению времени реагирования, такие как программа доверенных уведомителей. В дополнение к этим мерам мы можем также рассмотреть проактивные меры, включая проактивный мониторинг до получения сообщения и некоторые дополнительные правила на момент регистрации, такие как кружок или указатель слева.

А по результатам отчета INFERMAL можно будет рассмотреть ограничение массовой регистрации API или сроки проверки информации о пользователях. Следующий слайд, пожалуйста. Теперь перейдем к следующей части. Сначала мы хотели бы пригласить Мартина из CZ NIC для презентации принимающей страны. Так что, Мартин, слово за вами.

MARTIN KUNC

Спасибо. Я здесь, чтобы поделиться нашим опытом борьбы с фишингом в Чехии. Следующий слайд, пожалуйста. Немного о наших проектах, возможно, вы о них знаете. Наиболее важными, я думаю, могут быть Routing Demon Bird и ветка регистратуры. Возможно, вы также знаете о наших продвинутых измерениях DNS, которые мы называем ADAM, о сервере NodeDNS и маршрутизаторе TURRIS.

Следующий слайд, пожалуйста. Итак, кто мы такие, CZ. NIC — это регистратура домена .cz, которая также управляет Национальной CSIRT или CSIRT.cz, и я работаю в ней аналитиком по безопасности. Следующий слайд, пожалуйста. История началась в июне 2022 года, когда мы обнаружили очередной фишинговый сайт, что само по себе не было бы столь интересно, но на домене .cz это довольно необычно. Мы стараемся заботиться о нашем домене, и примерно в это же время появилась такая вещь, как жилищная субсидия.

Таким образом, государство выделяло субсидии, чтобы помочь гражданам, оказавшимся в тяжелой ситуации, получить дополнительные деньги на проживание. Следующий слайд, пожалуйста. Немного о персонажах фильма. У нас есть Министерство труда и социальных дел. Оно не играет здесь большой роли, но это просто для того, чтобы вы знали, что это за организация.

Следующий слайд, пожалуйста. Затем у нас есть нечто, что называется BankID. Я полагаю, что это не очень

распространено в других странах, но в Чешской Республике банки объединились и создали нечто под названием BankID, так чтобы вы могли использовать те же учетные данные, которые вы используете для доступа к своему банку, для доступа, скажем, к государственным сайтам. Так что в данном случае жертвами стали граждане, а затем появились злоумышленники.

Следующий слайд, пожалуйста. Сценарий этого фишинга довольно распространен. Люди получают SMS: «Смотрите, вы получите деньги, просто перейдите на этот сайт, который выглядит как сайт государственного учреждения, и вы не станете богатыми, но получите больше денег». Следующий слайд, пожалуйста. И таких случаев было довольно много.

Следующий слайд, пожалуйста. Как вы можете видеть, я понимаю, что вам очень сложно понять, что там написано, но в основном там говорится, что вам нужно просто нажать здесь, войти в систему и вы получите деньги. Следующий слайд, пожалуйста. После того, как вы нажмете на ссылку, вы попадаете на фишинговый сайт, который требует от вас входа с использованием вашего BankID. У нас есть другие вещи, другие типы аутентификации, которые вы можете использовать, но они специально запрашивают BankID, потому что есть очевидный способ злоупотребления этим.

И самое забавное, что это было возможно только в так называемое рабочее время. В Чехии был случай, когда

Чешская почта потеряла вашу посылку или что-то в этом роде, и вы могли зайти на сайт только в рабочее время. И если бы вы знали Чешскую почту, это показалось бы вполне нормальным, что у них сайт не работает круглосуточно, но в данном случае это было подозрительно, и им это было нужно именно потому, что злоумышленник использовал учетные данные в режиме реального времени и получил подтверждение с вашим вторым фактором аутентификации.

Следующий слайд, пожалуйста. Это один из примеров сайта. Он выглядит почти так же, за исключением URL-адреса, конечно. Следующий слайд, пожалуйста. Это еще один пример. Здесь вы можете выбрать банк. Не всегда можно было выбрать любой банк, но, по-видимому, они специально требовали некоторые, которые работают в данный момент. И если вы видите, в верхнем углу URL-адреса есть число, которое увеличивается каждый раз, когда пользователь нажимает на это. Так что мы можем получить некоторое представление о том, насколько успешна эта кампания.

Следующий слайд, пожалуйста. Это другой ракурс. Следующий слайд, пожалуйста. В 2022 году они начали с 11 доменов в месяц, что было все еще необычно и более чем достаточно, но не так уж и плохо. В феврале 2023 года у них было зарегистрировано 72 домена за один месяц, что было действительно много для нас, но в то время мы были готовы и брали их так быстро, как могли. Следующий слайд. Мы знали, что они со временем совершенствуются, и мы тоже хотели

совершенствоваться. Поэтому мы начали активный поиск, пытались улучшить процесс, изучали и делали заметки, потому что даже мелкие детали имели значение.

Следующий слайд, пожалуйста. Среди примеров активного поиска мы смогли провести поиск по зоне и увидеть домены, которые были зарегистрированы. Так что сначала мы попытались использовать похожие символы, которые были использованы для сайта, но, скорее всего, потому что им нужно было изменить и придумать новые идеи, новые названия, это оказалось не так полезно. Так что в конце концов мы решили просто посмотреть на домены, зарегистрированные на прошлой неделе, и это стало нашим источником информации. Следующий слайд, пожалуйста.

Это помогло нам составить список будущих фишинговых доменов, которые мы могли периодически сканировать. Это занимало около пяти минут. Каждые пять минут мы тестировали их и ни разу не получили отказ, ни разу наш IP-адрес не был заблокирован, так что они действительно не обращали внимания на наше сканирование. И как только мы обнаруживали, что фишинговый сайт запущен, мы получали уведомление на наши телефоны и были очень рады, что можем работать даже в нерабочее время, чтобы как можно быстрее его закрыть.

Я работал над этим вместе с Питером, так что я должен его здесь поблагодарить. Со временем нам удалось сократить

время на снятие сайта, что было очень важно в данном случае, как вы увидите позже на графиках. Следующий слайд, пожалуйста. Мы сделали заметки о том, что обнаружили. Схема была ясна: сайт всегда появлялся через несколько дней после регистрации, потому что сначала нужно зарегистрировать домен, настроить DNS-записи, получить сертификаты.

Когда все было готово, они активировали просмотр каталогов на этом сайте и загрузили zip-файл. В этот момент мы смогли несколько раз извлечь zip-файл с сайта и проанализировать его. Образцы иногда были одинаковыми, а иногда отличались, так как злоумышленники совершенствовали свою игру. После этого они распаковали zip-файл, и сайт заработал. Следующий слайд, пожалуйста.

Так что, если вам интересно, транспарентность сертификатов — это действительно важная вещь. Мы не только смогли найти субдомен в качестве панели администратора, где не требовался пароль и где мы могли видеть все, но и злоумышленник мог видеть все созданные сессии. Но транспарентность сертификатов в настоящее время помогает нам находить домены, которые не находятся в зоне .cz и которые мы не можем увидеть заранее. Следующий слайд, пожалуйста.

В конце концов, мы считаем это победой, потому что они прекратили свои попытки сразу через месяц после крупной

атаки, зарегистрировав в марте всего 28 доменов по сравнению с 72 в феврале.

С тех пор мы не видели ничего, что можно было бы сравнить с этим по масштабам. Конечно, были несколько попыток с другими TLD и отдельными доменами, но ничего подобного по масштабам. Следующий слайд, пожалуйста. Это может быть немного сложно понять, но я постараюсь объяснить. Зеленый цвет здесь обозначает запросы, которые не были правильно обработаны. Обычно они бы отображались красным цветом, но в данном случае они зеленые, потому что мы рады, что они не были обработаны, так как это фишинговые домены, доступ к которым мы смогли заблокировать.

Черные — это те, которые были обработаны. Важно отметить, что это не реальное количество пользователей, конечно, потому что мы не видим, сколько пользователей находится за одним резолвером, но это дает нам хотя бы приблизительную оценку и показывает, как мы продвигаемся и как мы справляемся с ними. Следующий слайд, пожалуйста. По сравнению с этим, здесь ситуация намного лучше. Как вы можете видеть, зеленые графики здесь намного сильнее, так что мы считаем это своего рода победой и тем, что мы действуем правильно и совершенствуемся.

Следующий слайд, пожалуйста. Информация о внутренних правилах: в наших правилах есть статья 17, которая позволяет нам удалять из зоны домены, которые, по нашему мнению,

нарушают кибербезопасность. В этом случае мы присваиваем им статус «вне зоны», который может сохраняться в течение одного месяца, что дает нам достаточно времени, чтобы владелец домена мог связаться с нами и объяснить, что происходит, и что это я, и что это должно было произойти.

Так что, если мы делаем что-то не так, мы можем это исправить и улучшить. Мы также публикуем список заблокированных доменов. Следующий слайд, пожалуйста. На этом я закончил. Надеюсь, вам понравилось, и у вас есть вопросы.

TOMONORI MIYAMOTO Спасибо, Мартин, за то, что поделился опытом в Чехии. А теперь давайте перейдем к вопросам и ответам. Есть вопросы? А, Габриэль. Да.

GABRIEL ANDREWS Здравствуйте, это Габриэль Эндрюс (Gabriel Andrews), для протокола. Спасибо большое за презентацию, Мартин. Мне было очень интересно, и я был действительно впечатлен, когда вы говорили о том, что вы обнаружили регистрацию подозрительных доменов, но, как я понял, вы еще не видели, что были созданы фишинговые сайты, но начали отслеживать эти домены и устанавливать правила для проверки и оповещения. Если я правильно понял, это очень проактивный подход, но мне интересно, считали ли вы, что нужно подождать, потому что вам нужно было собрать определенное

количество доказательств, прежде чем принимать меры? Не могли бы вы немного подробнее рассказать об этом?

MARTIN KUNC

Да, именно так. В то время мы действительно ждали доказательств. У нас было что-то, что могло бы нас выручить в случае блокировки домена, чтобы не помешать какому-то исследовательскому проекту или чему-то еще, что было бы нехорошо, и в этом случае мы действительно хотели подождать. И даже наш процесс настроен таким образом, что, если мы создаем файл и регистрируем доказательства, сайт в этот момент все равно должен быть доступен, пока не наступит момент его блокировки.

GABRIEL ANDREWS

Я могу только сказать, что, по-моему, никогда не видел такого проактивного подхода, или, по крайней мере, не слышал о таком проактивном поведении раньше. Я считаю, что это действительно впечатляет и очень интересно. Я знаю, что в прошлом были трудности с моим собственным сообщением о доменах, которые, по нашему мнению, будут использоваться в будущем, но у вас еще нет доказательств, и было довольно сложно найти баланс.

И тот факт, что вы смогли установить эти правила для самоконтроля и проявить дополнительную инициативу, чтобы сразу же обнаружить, когда они зарегистрированы или

настроены для фишинга. Это действительно здорово, и, возможно, здесь есть чему поучиться. Спасибо.

MARTIN KUNC Спасибо. Добавлю, что это была единичная фишинговая кампания, так что мы смогли увидеть важные узлы и обнаружить домены, которые будут использоваться для фишинга. В противном случае, если бы это был новый вид фишинга, нам нечего было бы отследить. Спасибо.

TOMONORI MIYAMOTO У нас Эшвин.

ASHWIN SASONGKO SASTROSUBROTO Да, спасибо. Эшвин, из Индонезии, для протокола. Спасибо обоим докладчикам за презентации. Я хотел бы задать несколько вопросов. Насколько эффективно использование активации DNSSEC, безопасного DNS, на веб-сайтах, а также использование сертификации ISO IEC 27001?

Может ли это помочь в борьбе со злоупотреблениями DNS, или это просто не работает? И во-вторых, от докладчика из SEC .cz, обычно вы приводите много примеров фишинга и так далее. Они обычно используют домены ccTLD .cz, или они используют gTLD .com или что-то еще? Спасибо.

MARTIN KUNC Я не уверен, что правильно понял первый вопрос, так что, пожалуйста, повторите его. Но что касается этого, то здесь речь шла конкретно о домене .cz, так что нам было проще разобраться, но у нас есть случаи, когда используются и другие домены, но не в таком большом количестве, скажем.

ASHWIN SASONGKO SASTROSUBROTO Да, первый вопрос на самом деле заключается в том, что на веб-сайте ICANN нас всегда призывают активировать DNSSEC. Насколько эффективна активация DNSSEC для борьбы со злоупотреблениями DNS? Кроме того, Индонезия, как и многие другие страны, является членом ISO и IEC, и вместе мы разработали стандарт ISO IEC 27001, который представляет собой систему управления безопасностью. Мне хотелось бы узнать ваш опыт. Насколько эффективна эта сертификация, 27001, против злоупотребления DNS. Спасибо.

MARTIN KUNC Хорошо, так что DNSSEC совершенно не помогает против фишинга. Я просто не вижу, как это может работать. А что касается стандарта ISO, то я не могу ответить на этот вопрос, потому что это далеко не моя область. Извините.

TOMONORI MIYAMOTO Следующая Адеронке. Извините за мое плохое произношение, но да, Вам слово.

ADERONKE ADENIYI

Здравствуйте. Спасибо, Мартин. Мой вопрос к Мартину. Ваша презентация, как уже сказал предыдущий докладчик, была замечательной, для меня она нова. Для протокола, меня зовут Адеронке, я из Нигерии. Мой вопрос касается BankID.

При попытке бороться со злоупотреблениями DNS вы рассматривали возможность сотрудничества с банковским регулятором, потому что у нас в Нигерии есть нечто подобное, называемое Bank Verification Number (Банковский верификационный номер), что охватывает все банки, включая платформы цифровых услуг. Я просто хотела бы знать, работали ли вы в какой-то момент с регулятором финансовых услуг или с эмитентом BankID? Спасибо.

MARTIN KUNC

Да, так что с моей точки зрения, нам не особо удалось до них достучаться, но, к счастью, они взяли дело в свои руки и начали информировать пользователей об этих попытках фишинга, используя свои приложения для рассылки уведомлений. Так что, я думаю, они делают все, что в их силах.

TOMONORI MIYAMOTO

Хорошо, спасибо. А теперь мы хотели бы перейти к следующей части. Мы хотели бы пригласить Карен и Грега из Interisle для

презентации о масштабах и распространении фишинга. Так что слово вам.

KAREN ROSE

Спасибо, добрый день. Я Карен Роуз (Karen Rose), а это Грег Аарон (Greg Aaron), мы из Interisle Consulting Group. Грег и я имеем 25-летний опыт работы в сфере доменных имен и очень рады возможности выступить перед вами сегодня. В течение последних пяти лет Interisle исследовала различные аспекты злоупотребления интернет-ресурсами при совершении киберпреступлений. Сегодня нас попросили сосредоточить внимание на злоупотреблениях DNS в связи с фишингом. Однако более широкий взгляд на проблемы злоупотребления ресурсами вы можете найти в наших опубликованных отчетах. Время ограничено, поэтому перейдем сразу к делу. Так что, пожалуйста, следующий слайд. К сожалению, суть в том, что фишинг и злоупотребления DNS растут с поразительной скоростью. Только за последние 12 месяцев было выявлено более 2 миллионов фишинговых атак и 1,5 миллиона уникальных фишинговых доменов, что на 425% больше, чем за предыдущий квартал, и на 425% больше, чем за предыдущий год.

И это значительно занижает масштаб проблемы, так как многие атаки просто не регистрируются. 77% этих фишинговых доменов были специально зарегистрированы с целью проведения кибератак. Фишинг наносит высокий

ущерб обществу. Каждую минуту прямые финансовые потери составляют более 18 000 долларов. И это значительно занижает масштаб проблемы, так как большинство потерь не регистрируется, особенно на глобальном уровне. Я думаю, что из этого роста мы должны сделать вывод, что усилия по борьбе со злоупотреблениями DNS на сегодняшний день в основном неэффективны. И если вам интересно, что означает этот спад примерно в середине графика, то это связано с закрытием компании Freenum, которая была очень лояльной к фишингу доменной компанией. Закрытие Freenum на некоторое время выбило фишеров из колеи, но, как вы видите, они быстро пришли в себя, и уровень злоупотреблений снова вырос.

Следующий слайд, пожалуйста. При регистрации доменных имен фишеры, как правило, используют две вещи: низкие цены и простоту регистрации. Идеальным вариантом для фишеров являются доменные имена по цене около 2 долларов или меньше. И именно такие цены очень распространены в новых gTLD, которыми фишеры пользуются в непропорционально больших масштабах. Если вы посмотрите на верхнюю диаграмму, то увидите, что общая доля рынка новых gTLD, этот маленький желто-красный сектор, составляет всего 11 %. Однако если вы посмотрите на нижний график, то увидите, что на долю новых gTLD пришлось более 51 % всех фишинговых доменов за последний год. При этом домены .com и .net также остались весьма привлекательными

для фишеров, на них приходится 32 % всех фишинговых доменов. Один из способов, с помощью которого фишеры могут дешево получить доступ к доменам .com и .net, — это бесплатные рекламные акции и пакетные предложения хостинга, предлагаемые некоторыми регистраторами. Фишеры также используют простую процедуру регистрации и выбирают TLD и регистраторов, которые предъявляют мало требований и проводят мало проверок данных.

Мой коллега Грег расскажет о массовой регистрации через минуту. Фишеры также имеют предпочтительных поставщиков, регистраторов и TLD, которые сочетают в себе дешевизну и простоту. Компании, которые чаще всего становятся жертвами злоупотреблений, как правило, входят в пятерку или десятку лидеров из года в год. Сегодня у нас нет времени, чтобы перечислить все эти компании, но вы можете найти их в некоторых наших последних отчетах. Следующий слайд, пожалуйста. Фишеры часто регистрируют имена по шаблонам, и часто эти шаблоны очень заметны и легко обнаруживаются. Я привела здесь несколько примеров из реальных кибератак. Слева вы видите одну из тактик — алгоритмически сгенерированные имена, которые часто являются вариациями одной темы или даже полностью случайными строками символов.

Имена, которые очень похожи на бренды, чтобы обмануть ничего не подозревающих потребителей, а фишеры часто используют одни и те же регистрационные данные снова и

снова или даже явно ложную и поддельную информацию. Однако для выявления таких злоумышленных схем можно использовать автоматизированные инструменты. Некоторые ccTLD уже имеют специальные системы DNS для проверки, а также существуют коммерческие инструменты для таких задач, как проверка адресов. Следующий слайд, пожалуйста.

GREG AARON

Каждый год мы изучаем, как регистрируются эти домены, и когда фишеры и другие преступники регистрируют доменные имена, они обычно не регистрируют только одно или два за раз. Они очень часто регистрируют целые наборы. И, как сказала Карен, они обычно следуют определенной схеме, так что их легко вычислить. Но вы можете увидеть их, если посмотрите на наборы доменов, зарегистрированных один за другим, например, у определенного регистратора.

По крайней мере 37% доменов, используемых для фишинга, зарегистрированы пакетами. И наша методология занижает их количество. Мы видим, какие из них использовались для фишинга, мы видим, что они связаны между собой, но в этих пакетах есть и другие домены, которые мы не нашли и не зафиксировали просто потому, что иногда очень сложно собрать данные. Иногда эти пакеты бывают очень большими. В прошлом году мы обнаружили один пакет, в который входило более 17 000 доменов, использованных одним злоумышленником.

Идея в том, что фишеры, особенно сейчас, действуют очень быстро. Жертвы появляются в течение первых восьми часов после запуска фишингового сайта. Так что фишеры предполагают, что их поймают, что их доменное имя может быть заблокировано в определенный момент, но у них есть другие домены. Одна из причин, по которой мы видим все больше и больше используемых доменов, заключается в этой автоматизации.

Они готовы перебирать множество доменов и продолжать свои атаки, и пока они могут получать прибыль и поддерживать эти сайты в рабочем состоянии в течение некоторого времени, они продолжают действовать. Мы видим так много фишинга, потому что он успешен. Так что мы должны подумать о том, почему это происходит, почему мы наблюдаем постоянную смену доменов. Следующий слайд, пожалуйста.

KAREN ROSE

Так что злоупотребления DNS становятся возможными благодаря выбору. Выбору, который делает ICANN в своих политиках и бизнес-стандартах, определяющих функционирование рынка, и выбору, который делают компании при ведении своего бизнеса. Мы часто слышим мантру о том, что конкуренция — это хорошо, так что просто увеличение конкуренции должно быть еще лучше, верно? Но с экономической точки зрения это не всегда так.

В отсутствие разумных правил чрезмерная конкуренция может иметь негативные последствия. Злоупотребления DNS и киберпреступность, которую они подпитывают, подобны загрязнению окружающей среды в других отраслях. Это негативный экономический эффект, который ложится на плечи потребителей и общества. Сегодня рынок DNS является весьма конкурентным. Существует более 2000 регистраторов, сотни открытых gTLD, а для киберпреступников доменные имена являются расходным товаром. Они практически взаимозаменяемы и могут быть произведены отраслью практически с нулевыми маржинальными издержками.

Так что в отсутствие эффективной политики противодействия злоупотреблениям преступники сегодня очень легко эксплуатируют эту динамику рынка и имеющиеся возможности. Мы считаем, что нам действительно нужны разумные, проактивные меры, которые помогут пресекать злоупотребления доменами до того, как они произойдут, а не просто смягчать последствия после того, как ущерб уже нанесен, хотя более эффективные меры смягчения всегда будут полезны.

И важно сделать это сейчас и реализовать политику сейчас, потому что по мере появления на рынке новых gTLD, потенциально с новыми раундами gTLD, это будет оказывать дальнейшее понижательное давление на цены доменов и усиливать конкурентное давление на рынке. И если ничего не

изменится, этот график будет продолжать расти вверх и вправо. Следующий слайд, пожалуйста.

GREG AARON

Одна из тенденций, которую мы наблюдаем, особенно в Европе, заключается в том, что операторы регистратур делают что-то новое. Некоторые из них, например, не требуют от всех владельцев доменов подтверждать свою личность заранее, но используют подходы, основанные на оценке рисков. Например, мы видели, как несколько операторов регистратур заявили, что массовая регистрация доменов является примером риска.

К нам приходят владельцы доменов, мы не знаем, кто они, но они регистрируют очень много доменов. Так что, возможно, нам следует попросить их подтвердить свою личность и, возможно, не разрешать эти домены для разрешения и работы, пока мы не будем уверены в том, кто они. Так что это подход, основанный на оценке рисков, который сейчас применяется в некоторых европейских TLD. Текущие требования ICANN к проверке очень минимальны.

И на самом деле, одно из недавних мероприятий ICANN по обеспечению выполнения договорных обязательств показало, что 20% прошедших проверку регистраторов не выполняли минимальные требования по проверке. Так что мы видим в этом возможность рассмотреть подходы, основанные

на оценке рисков, проводить проверку и принимать превентивные меры, что усложнит жизнь преступникам.

Следующий слайд, пожалуйста. Итак, наши идеи для обсуждения включают усиление требований к проверке и рассмотрение проблем массовой регистрации. И эти две вещи, кстати, могут идти рука об руку. Еще один факт, о котором вы, возможно, не знаете, заключается в том, что договоры ICANN требуют от операторов регистратур вести дела со всеми без исключения регистраторами, аккредитованными ICANN. За этим стоит веская причина. Люди не хотели, чтобы компании вытесняли друг друга, мы хотим конкурентоспособных и равных условий для всех вовлеченных компаний.

Однако регистратуры по-прежнему обязаны вести дела с регистраторами, которые приносят им много проблем. Мы предлагаем рассмотреть эту ситуацию, поскольку она иногда ставит регистратуру в невыгодное положение и заставляет ее оставлять плохое впечатление из-за притока проблемных владельцев доменов. Так что, возможно, здесь мы можем что-то сделать.

И, конечно же, регистратуры и регистраторы располагают инструментами. Некоторые из них экспериментируют с системами, позволяющими выявлять злоумышленные домены до того, как они появятся, и на этой неделе ведутся дискуссии по поводу таких решений. Так что мы хотим оставить вас с

мыслью о том, что существуют некоторые инструменты и решения, а также, возможно, некоторые политики, которые могут улучшить ситуацию. Следующий слайд, пожалуйста.

KAREN ROSE

Итак, у нас есть несколько новых отчетов с данными за третий квартал этого года, так что следите за их появлением. Если вы хотите ознакомиться с нашими отчетами, повторюсь, мы не просто анализируем доменные имена, мы также изучаем такие вещи, как злоупотребления и хостинг, злоупотребления и субдомены, а некоторые из наших исследований также касаются фишинга, спама и вредоносных программ. Так что мы приглашаем вас ознакомиться с нашими отчетами, а вот и веб-сайт.

Наши источники данных, методология и дополнительные данные находятся на нашем веб-сайте под названием Cybercrime Information Center (Центр информации о киберпреступности), который является проектом Interisle. Там вы найдете обширные данные и рейтинги, если захотите ознакомиться. Мы также присутствуем на Substack и публикуем записи в блоге каждые несколько дней, пару раз в неделю, так что загляните туда, и, конечно же, на наш веб-сайт, и мы будем рады обменяться с вами информацией по электронной почте. Спасибо большое.

TOMONORI MIYAMOTO Спасибо, Карен и Грег, за вашу презентацию. И, чтобы не затягивать время, давайте перейдем к следующей части. Если у вас есть вопросы, пожалуйста, отметьте их, чтобы мы могли обсудить их позже в ходе этого заседания. Так что я передаю слово Яношу. Пожалуйста.

JANOS DRIENYOVSZKI Спасибо, Томо. А теперь мы хотели бы перейти к следующим шагам в области разработки политики и потенциальных микро-PDP или процессов разработки политики, которые могли бы решить обсужденные вопросы. Я хотел бы предоставить слово Грэму из NetBeacon для его презентации.

GRAEME BUNTON Спасибо. Доброе утро всем. Меня зовут Грэм Бантон (Graeme Bunton). Я исполнительный директор Института NetBeacon. Институт NetBeacon является частью регистратуры доменов общественного характера, которая управляет TLD .org в целях выполнения своей некоммерческой миссии общественного блага. Совсем недавно, примерно две недели назад, мы опубликовали документ, в котором предложили пять потенциальных идей для PDP, которыми мы хотели бы поделиться с сообществом. У меня не так много времени, так что я не буду вдаваться в подробности этих идей для PDP. Я предоставлю ссылку на полный текст документа, который, я уверен, вам понравится. Но здесь я только вкратце расскажу о нем. Следующий слайд, пожалуйста. Краткая информация о

том, почему мы проделали эту работу. Институт NetBeacon каждый день занимается вопросами сокращения злоупотреблений DNS. Но мы также являемся стороной, связанной договорными обязательствами, и поэтому у нас есть относительно уникальная точка зрения. Мы во многом выполняем работу, очень похожую на работу InterIsle, где у нас есть проект по измерению и пониманию злоупотреблений DNS в экосистеме под названием NetBeacon Map (карта NetBeacon). Мы также управляем централизованной службой сообщения о злоупотреблениях под названием NetBeacon Reporter (репортер NetBeacon), где мы видим десятки тысяч злоумышленных доменных имен, проходящих через нее каждый день. Итак, основываясь на этих данных и этих идеях, мы хотели предоставить... Помедленнее. Да, извините, слишком быстро.

Мы хотели посмотреть, сможем ли мы поддержать дискуссии в сообществе, чтобы выдвинуть некоторые идеи, которые, по нашему мнению, могут быть реализованы в кратчайшие сроки, оказать постепенное влияние на проблемы злоупотребления DNS и действительно показать этому сообществу, что, по нашему мнению, могут означать PDP с узкой сферой действия.

Следующий слайд, пожалуйста. Я не буду вдаваться в подробности. Вкратце, проверка связанных доменов — это обязанность регистраторов реагировать на сообщения о злоупотреблениях. Они получают хорошо подтвержденное, подлежащее действию сообщение о злоупотреблении в

отношении вредоносного доменного имени. Регистратор обязан проверить, есть ли другие доменные имена, связанные с этим доменным именем, и принять меры, если есть доказательства злоупотребления.

Следующий слайд, пожалуйста. API с ограниченным доступом; одним из ключевых выводов отчета ICANN INFERMAL, и за этот отчет большое спасибо ICANN OCTO, было то, что API с неограниченным доступом составляли, я думаю, 401%. Так что у регистратора с неограниченным доступом к API вероятность злоупотребления была на 401% выше. И что мы можем с этим сделать? Как мы можем создать препятствия, прежде чем владельцы доменов получат доступ к таким инструментам, которые позволяют осуществлять массовую регистрацию?

Следующий слайд, пожалуйста. Контакты по вопросам злоупотребления субдоменами. Это предложение о том, чтобы обязательства по предотвращению злоупотребления DNS, существующие на уровне регистраторов, были распространены на владельцев доменов, которые предоставляют субдомены третьим сторонам.

Следующий слайд, пожалуйста. Механизмы защиты владельцев доменов. В условиях, когда регистратуры и регистраторы прилагают все усилия для борьбы со злоупотреблениями DNS в широких масштабах, ошибки неизбежны. И мы должны обеспечить владельцам доменов, пострадавшим от мер по борьбе со злоупотреблениями,

четкий механизм устранения допущенных ошибок. Следующий слайд, пожалуйста. Бот-сети и координация DGA. В настоящее время для пресечения ботнетов и алгоритмов генерации доменов правоохранительные органы обычно вынуждены обращаться в каждую регистратуру отдельно, что является неэффективным.

Итак, мы предлагаем создать в ICANN централизованную функцию для сбора и распространения информации, а также повышения эффективности борьбы с ботнетами. Следующий слайд, пожалуйста. Я мог бы довольно долго говорить о каждом из этих потенциальных PDP, и с удовольствием сделаю это, если вы подойдете ко мне в перерыве.

Но я думаю, что для этой аудитории есть несколько ключевых выводов, которые я хотел бы сделать, а именно: сейчас есть реальная возможность продвинуться вперед в этом сообществе по PDP, по разработке политики, чтобы реально изменить ситуацию со злоупотреблениями DNS. Но мы действительно должны обеспечить, чтобы все мы были коллективно привержены осуществлению узконаправленных процессов, ограниченных конкретными проблемами. Никто не может получить все, что хочет. Для достижения прогресса потребуется сфокусированность. Для своевременного прогресса потребуется очень интенсивная концентрация. Эти вопросы сложны, поскольку мы вникаем в детали потенциальных идей, которые сообщество может принять.

Есть реальные операционные последствия, есть реальные проблемы, которые необходимо решить, но мы можем добиться некоторых побед. Мы можем добиться небольших, постепенных, своевременных побед, и это лучше, чем ничего. Я думаю, что размер куска, который мы откусываем, напрямую зависит от того, сколько нам придется жевать. И я думаю, что мы действительно хотим посмотреть, сможем ли мы заставить это сообщество откусить несколько маленьких кусочков, пережевать их и получить хороший результат, своевременно изменив ситуацию со злоупотреблениями DNS.

И последнее, что я хотел бы подчеркнуть, основываясь на том, что сказал Interisle о моделях злоупотребления DNS, это то, что тематически нам нужно перейти от отдельных сообщений о злоупотреблениях к решению проблемы злоупотребления DNS в масштабе. Так что поправки к договорам, внесенные в прошлом году, являются отличным шагом. В наших данных мы постоянно видим, как регистратуры и регистраторы приостанавливают действие вредоносных доменных имен. Но обязательства лежат на уровне индивидуальных сообщений о злоупотреблениях.

Итак, два наших предложения, первые два, проверка связанных доменов и ограничение доступа к массовому API, направлены на то, чтобы понять, можем ли мы разумно и ответственно перейти к решению проблемы злоупотреблений не только на уровне индивидуальных сообщений, но и в масштабах кампаний по злоупотреблениям. И даже если это

не самые правильные идеи, я думаю, что именно так сообщество должно думать о том, как бороться со злоупотреблениями в будущем. Итак, с нашей точки зрения, опубликовав этот документ, мы достигли своих целей.

Сообщество обсуждает идеи, обсуждает ограниченные идеи, идеи, которые, по нашему мнению, могут быть успешными. И даже если это не эти идеи, они правильно ограничены. И именно это мы хотели бы продолжать видеть в этом сообществе. Мы надеемся, что сообщество продолжит обсуждать и продвигать подобные идеи. Спасибо большое за возможность быть здесь сегодня. Я очень ценю это.

NICO CABALLERO

Спасибо вам большое, Грэм. Прежде чем снова передать слово Томо, я хотел бы попросить уважаемых представителей GAC принять во внимание необходимость принятия быстрых мер, учитывая тот факт, что в этот самый момент за нами наблюдают злоумышленники. Так что если мы разработаем PDP и через пять лет решим... они уже будут на два-три шага впереди нас. По моему скромному мнению, нам действительно следует действовать быстро. Снова к вам, Томо.

JANOS DRIENYOVSZKI

Спасибо, Нико. Теперь перейдем к тому, на чем, по нашему мнению, GAC следует сосредоточить внимание в плане

потенциальных узконаправленных PDP. Прежде чем перейти к своей презентации, я хотел бы также быстро пройтись по идеям, представленным вчера на заседании Палатой сторон, связанных договорными обязательствами. Одна из идей заключалась в том, чтобы ввести требование о составлении отчета о злонамеренно зарегистрированных доменах, на основании которого можно было бы принять меры. Это привело бы к блокированию других злонамеренно зарегистрированных доменов в учетной записи того же владельца домена. Вторая идея заключалась в потенциальной поправке к договору, которая гарантировала бы, что регистраторы, предлагающие API или программу для реселлеров, имеют необходимые договорные средства для наложения на своих реселлеров требований по борьбе со злоупотреблениями DNS.

Третья идея заключалась в разработке оперативной структуры для предоставления всем операторам регистратур gTLD проверенного списка доменных имен, созданных ботнетами. И четвертая идея заключалась в разработке передовой практики для сообщения о фишинге с целью повышения качества сообщений. Теперь, переходя к тому, на чем, по нашему мнению, должен сосредоточиться GAC, или к идеям, которые следует обсудить более подробно, сегодня много говорилось о проактивных мерах и, в частности, о массовых регистрациях.

Мы сейчас находимся на этапе изучения широкого спектра полезных проактивных мер, а также мер по смягчению последствий или реактивных мер. Но если цель, как уже упомянул Нико, состоит в том, чтобы быстро достичь чего-то значимого, в частности, до начала нового раунда gTLD, то следует определить приоритетность некоторых конкретных действий, что также связано с тем, о чем говорил Грэм в отношении очень узких и целенаправленных PDP.

В коммюнике GAC из Сиэтла было предложено рассмотреть вопрос о массовой регистрации доменных имен как один из наиболее значимых факторов, способствующих злоупотреблениям DNS, в том числе в соответствии с упомянутым отчетом INFERMAL. Конечно, как было показано сегодня утром, массовая регистрация доменов сопряжена с более высоким риском злоупотребления DNS, а ее последствия также более серьезны по сравнению с отдельными злоумышленными доменами.

Исследование INFERMAL также показало, что более строгие правила регистрации и проактивные меры проверки могут способствовать борьбе со злоупотреблениями DNS. Таким образом, очевидно, что в процесс массовой регистрации доменов следует ввести некоторые дополнительные ограничения. Мы считаем, что одним из вариантов в этом направлении могло бы быть требование к сторонам,

связанным договорными обязательствами, принимать проактивные меры в отношении массовой регистрации.

Это может включать ограничение массовой регистрации API, например, путем ограничения доступа к API известным или проверенным пользователям на основе проверки личности, деятельности или репутации владельца домена, как это было предложено Грэмом в его презентации. Мы считаем, что эта идея является одной из наиболее реалистичных для достижения консенсуса в краткосрочной перспективе. Могут также быть введены более высокие цены на массовую регистрацию доменов, отсрочка регистрации или ограничение объемов регистрации и т. д.

Такие проактивные меры будут дополнять реактивные меры или меры по смягчению последствий, изложенные также в предложении Палаты сторон, связанных договорными обязательствами, по направлению отчетов, на основании которых могут быть приняты меры, а также в предложении NetBeacon по проверке связанных доменов и принятию соответствующих мер при подтверждении злонамеренной регистрации. Так что мы достигли бы таким образом сочетания проактивных и реактивных мер в отношении массовых регистраций.

Теперь перейдем к другим возможным проактивным мерам и мерам по смягчению последствий. Как в Гамбургском коммюнике, так и в Сиэтлском коммюнике GAC вновь

подчеркнул важность проактивного мониторинга, а также упомянул проактивные методы борьбы со злоупотреблениями DNS и связь между борьбой со злоупотреблениями DNS и работой над регистрационными данными доменных имен. GAC призвал регистраторов изучить возможность использования систем обнаружения злоупотреблений DNS на основе искусственного интеллекта.

В этом отношении мониторинг и поведение при регистрации могут стать еще одной областью для изучения. Это означало бы выявление индикаторов злоумышленной регистрации, которые вызывали бы реакцию сторон, связанных договорными обязательствами, либо во время регистрации, либо вскоре после нее. Эта мера соответствовала бы первой рекомендации отчета малой группы по злоупотреблениям DNS, представленного Совету GNSO в октябре 2022 года. Это означало бы, что все регистрации, представляющие определенный уровень риска злоумышленной регистрации, должны проходить проверку идентичности.

Здесь мы имеем примеры проактивных практик из сферы ccTLD в Европе, которые предполагают использование систем обнаружения злоупотреблений DNS на основе искусственного интеллекта. Другой мерой может быть также периодическая проверка в течение жизненного цикла доменного имени. Так что это означало бы проверки при продлении или передаче домена. И на этом я хотел бы предоставить слово Сьюзан.

SUSAN CHALMERS

Спасибо, Янош. Я кратко остановлюсь на третьей идее для PDP, которая обсуждалась ведущими по темам GAC, а именно на обязательствах по представлению отчетности. Так, разумная политика строится на фактах, на релевантных фактах, которые GAC может учитывать при разработке политики в отношении злоупотреблений DNS. ICANN включает в свою работу информацию с платформ измерения, таких как те, что предоставляются ICANN, Domain Metricon, Институтом NetBeacon.

Мы также можем обратить внимание на отчеты о киберпреступности, подготовленные такими компаниями, как Interisle, о которой мы сегодня слышали, а также на отчет INFERMAL, который широко обсуждался в Сиэтле во время ICANN82 и также является релевантным доказательством. Отдел ICANN по контролю исполнения договорных обязательств ежемесячно публикует отчеты о злоупотреблениях DNS, которые являются хорошим доказательством, которое может послужить основой для разработки эффективной политики, и мы имеем хорошее представление о том, как стороны, связанные договорными обязательствами, реализуют обязательства по предотвращению злоупотреблений DNS 2024 года, благодаря отчетам о выполнении договорных обязательств.

Но у нас нет полной картины. Нет требований к сторонам, связанным договорными обязательствами, публично сообщать о своей деятельности по борьбе со злоупотреблениями DNS или о реализации поправок. Так что вот одна идея. Таким образом, можно сосредоточиться на отчетности о статистике злоупотреблений для сторон, связанных договорными обязательствами. Это просто еще одно предложение, которое можно добавить к списку идей, о которых мы слышали вчера и сегодня.

Следующий слайд, пожалуйста. Так что, это следующие шаги и направления действий ICANN в области политики. Если вы участвовали в вебинаре, который мы организовали перед ICANN-83, вы слышали от малой группы GNSO о злоупотреблениях DNS. Эта малая группа уже приступила к работе. Их задача, в основном, состоит в оценке усилий по борьбе со злоупотреблениями DNS, предпринятых на сегодняшний день, и определении необходимости дальнейшей работы над политикой. Проект выводов и рекомендаций должен быть представлен в сентябре этого года, а итоговый отчет — в октябре.

Мы понимаем, что этот срок может быть сокращен, но я не буду говорить от имени малой группы по злоупотреблениям DNS сегодня. Я просто хочу, чтобы представители GAC знали, что эта работа ведется в GNSO. Сегодня у нас запланировано двустороннее совещание с Правлением, и я прошу персонал поддержки перейти к вопросу, который мы им предложили.

Так что мы обсудим это с Правлением. Я думаю, что, если вы обратитесь к любому сотруднику ICANN, любому коллеге, скорее всего, он согласится, что PDP должны проходить в более короткие сроки. Некоторые PDP занимают годы.

Я думаю, что вопрос, который мы поставим перед Правлением, заключается в том, как, и это не относится конкретно к злоупотреблениям DNS, но как мы можем стимулировать радикальные изменения в процессах PDP, чтобы мы могли быстро увидеть результаты? Не через 10 лет, не через пять лет, не через три года, а как насчет 12 месяцев или меньше? Это то, на что я бы хотела обратить внимание представителей GAC сегодня. Спасибо.

Давайте вернемся назад. Многие представители GAC знакомы с тем, как представители GAC могут участвовать в изменении политики ICANN и способствовать его реализации. Для тех, кто не знаком с этим процессом, я хотела бы очень кратко рассказать о некоторых из этих путей. Первый — это процессы разработки политики, на которых мы сегодня сосредоточили свое внимание. Мультистейкхолдерные процессы разработки политики в ICANN предполагают широкое участие заинтересованных сторон из всего сообщества ICANN, включая представителей GAC.

PDP приводят к консенсусной политике. Консенсусная политика становится частью договора и, таким образом, является обязательной для всех сторон. Следующим способом

изменения политики в ICANN могут быть поправки к договорам. Таким образом, политика может быть введена в действие посредством поправок к договорам между ICANN и регистратурами, а также между ICANN и регистраторами, но в отличие от мультистейкхолдерного процесса разработки политики, поправки обсуждаются на двусторонней основе.

Так что у нас был набор важных поправок 2024 года, касающихся злоупотреблений DNS, которые были введены в действие. Они вступили в силу 5 апреля прошлого года, если я не ошибаюсь. Эти поправки установили основополагающие обязательства для регистратур и регистраторов ICANN, но они были в основном результатом двусторонних переговоров. Был проведен процесс общественных комментариев по предложенным поправкам, но в отличие от PDP, заинтересованные стороны, которые не являются ни ICANN, ни сторонами, связанными договорными обязательствами, не принимали непосредственного участия в этом процессе.

Что касается представителей GAC, то, конечно, нашим основным инструментом являются рекомендации GAC и наша способность выработать консенсусные рекомендации для Правления ICANN. Рекомендации GAC, когда они хорошо продуманы и скоординированы, являются самым мощным инструментом GAC для осуществления изменений в политике ICANN. Так что я просто хотела дать этот краткий обзор, особенно для новых представителей GAC. Следующий слайд,

пожалуйста. Итак, я полагаю, у нас осталось 15 минут. Хорошо. Мы хотели бы сэкономить время для обсуждения GAC.

Так что председатель, как обычно, объявил о начале обсуждения вопросов перед заседанием ICANN83. А ведущие по теме злоупотребления DNS в GAC заранее предоставили текст для списка GAC. Здесь я выделила основные моменты из предоставленного нами текста. В разделе важных вопросов мы сможем обсудить ход заседания в части, касающейся злоупотребления DNS, в частности, в ходе заседания.

Мы предложили сосредоточить внимание на обзоре ситуации со злоупотреблениями DNS и вопросах борьбы с ними для PDP, а также на следующих шагах. Мы также предложили поощрять целенаправленные PDP с узкой сферой действия, которые позволяют достичь консенсуса в гораздо более короткие сроки. И мы хотели обсудить это с представителями GAC, представить это коллегам и открыть дискуссию.

NICO CABALLERO

Спасибо большое, США. Давайте вернемся, пожалуйста, к слайду № 12, последнему слайду. Да, вот здесь. Нет. Вот здесь. Итак, что касается разработки политики, и, прежде чем я предоставлю слово Индонезии, извините, что заставил вас ждать, или это старая рука, Ашвин? Это старая рука? Вы подняли руку. Так что, прежде чем я предоставлю вам слово и прежде, чем мы фактически откроем дискуссию для вопросов

или комментариев, очень важно учесть PDP, то есть процесс разработки политики для членов GAC.

Мы хотим убедиться, что вы чувствуете себя комфортно, что у вас есть возможность участвовать, я бы сказал, значимым образом, что вы чувствуете себя комфортно, что председательство на этих заседаниях, суть в том… какой смысл участвовать в процессе PDP, если у вас нет возможности высказать свое мнение, сказать все, что вы хотите сказать, если, например, и это всего лишь пример, я не говорю, что это происходит, но если председатель не является, я бы сказал, эффективным, ваши идеи не могут быть переданы, слово предоставляется кому-то другому, прежде чем вы можете высказать какие-либо вопросы во время этих PDP.

Идея заключается в том, чтобы, как я уже сказал в начале, вы чувствовали себя комфортно, участвуя в этих PDP. И, конечно, я полностью согласен с тем, что уже было сказано представителем США о том, что PDP должны быть короче, быстрее и гораздо более эффективными. С точки зрения правительства, мы не можем тратить два, три, четыре года или даже, я бы сказал, больше одного года, это не имеет большого смысла. Мне не нужно объяснять циклы работы правительств.

В некоторых странах президентский срок составляет четыре года. Обычно наши министры ИКТ или министры иностранных дел занимают свои должности два года, три года, один год. Конечно, это зависит от страны, но вы понимаете, о чем я,

верно? Так что, еще раз, извините, что заставил вас ждать, Индонезия, вам слово.

ASHWIN SASONGKO SASTROSUBROTO: Извините. Спасибо, Нико. На самом деле, мой вопрос такой же, как и мой последний вопрос к нашему другу из Чехии, о стандарте ISO IEC 27001, достаточно ли он силен для предотвращения злоупотребления DNS или каков ваш опыт в этом вопросе? Я задаю этот вопрос, потому что, во-первых, злоупотребления DNS являются большой проблемой в Индонезии, это очень большая проблема сегодня.

Во-вторых, Индонезия, конечно, и другие страны также являются членами ISO IEC. И в-третьих, ISO IEC имеет совместный комитет, который занимается ИКТ, и подкомитет 27, который специально занимается кибербезопасностью. Так что мое предложение состоит в том, что если стандарт 27 000 недостаточен для предотвращения злоупотребления DNS, то мы должны сообщить об этом организациям ISO IEC, у нас будет общее собрание в сентябре следующего года, и мы скажем им: «Послушайте, почему бы вам не пересмотреть стандарт 27 000?

Потому что там у них также есть так называемая политика разработки PDP DECO. И одно из направлений разработки политики заключается в использовании систем сертификации 27 000 для защиты нашей системы. Теперь, если опыт ICANN показывает, что этого недостаточно, то мы сообщим им об

этом и пересмотрим его или обсудим с ними все, что сможем. Даже вы, Нико, можете отправить письмо в IEC. Это не проблема, конечно. Спасибо.

NICO CABALLERO Спасибо, Индонезия. Принято к сведению. Следующий вопрос – Индия.

SUSHIL PAL Спасибо, председатель, и спасибо участникам дискуссии, особенно Interisle и NetBeacon за информативный доклад. Мы более чем довольны и полностью поддерживаем проведение более коротких и узконаправленных PDP. Однако я по-прежнему считаю, что мы сосредоточиваемся больше на симптомах, а не на причине. Мы рассматриваем взаимосвязь между массовым созданием, более низкой стоимостью, легкостью доступа и отсутствием злонамеренного использования доменных имен, и, на мой взгляд, это всего лишь симптомы, а не причины.

Я думаю, что причина заключается в достоверности данных WHOIS, а также в идентификации. Я хотел бы ответить участникам дискуссии по этому вопросу, потому что я просто провожу параллель с нашим физическим миром. Я думаю, что мы живем в физическом мире, но мы точно знаем, кто живет по соседству, верно? И я по-прежнему считаю, что эти

вредоносные доменные имена возникают только из-за анонимности.

Злоумышленники, владельцы доменов, не несут никакой ответственности, что фактически дает им возможность уйти в любой момент. Все, что мы можем сделать, это удалить доменное имя, и ничего больше, верно? Так что, проводя эту параллель, я не думаю, что увеличение стоимости с 2 до 10 или 20 долларов действительно приведет к сокращению числа вредоносных доменных имен, потому что выгода слишком велика, как мы видели, примерно 18 000 долларов в минуту.

Так что, на наш взгляд, необходимо ввести ответственность не только со стороны регистраторов, но и со стороны владельцев доменов. В то же время это будет означать дополнительные расходы для регистраторов и владельцев доменов, но я думаю, что мы должны искать такое решение. Спасибо.

NICO CABALLERO Спасибо, Индия. У нас есть семь минут и один, два, три, четыре, пять, шесть, семь, семь ораторов. Так что я бы хотел, очень просить вас быть краткими и переходить сразу к делу. Сьюзан, вы хотели бы что-нибудь сказать перед... Нет? Хорошо. Тогда я предоставляю слово Европейской комиссии. Вам слово.

GEMMA CAROLILLO Спасибо большое, Нико. Гемма Каролильо (Gemma Carolillo), Европейская комиссия. Спасибо коллегам из GAC, которые

организовали это очень информативное заседание с приглашенными докладчиками. Я хотела бы вернуться к вопросу о рассмотрении коммюнике и возможных дальнейших действиях. Так что, с нашей точки зрения, очень хорошо, что появился этот импульс.

Многие участники сообщества, похоже, заинтересованы в продвижении вперед в вопросе злоупотребления DNS после внесения поправок к договорам, что мы оцениваем очень, очень положительно. Мы видим это по деятельности Палаты сторон, связанных договорными обязательствами, по таким инициативам, как инициатива NetBeacon, о которой мы сейчас слышим.

Я думаю, что мы должны обязательно воспользоваться этим и сотрудничать с другими частями сообществ. Учитывая, что приоритетом для GAC всегда было принятие новых мер до начала нового раунда, мы также должны быть прагматичными и стремиться определить достижимые меры в рамках предоставленного нам времени. Это означает расстановку приоритетов, не забывая при этом об общей картине, а просто стремясь к приоритезации.

И с этой точки зрения мы считаем важным рассмотреть возможность вынесения рекомендаций, касающихся узконаправленных PDP, но мы бы предложили GAC также определить эти приоритетные темы. Сегодня мы услышали о возможности объединения некоторых проактивных мер,

таких как мониторинг моделей поведения при регистрации данных и массовой регистрации.

Мы видели, что на рассмотрении находится несколько предложений, которые, по нашему мнению, следует изучить, а также мы считаем важным рассмотреть обязательства по обеспечению транспарентности. Это было частью очень ранней позиции GAC, когда были проведены общественные комментарии по поправкам к договорам о злоупотреблениях DNS. Спасибо.

NICO CABALLERO Спасибо вам большое, Европейская комиссия. Я полностью с вами согласен. И, кстати, у нас будет шесть заседаний по подготовке коммюнике, так что у нас будет более чем достаточно времени для обсуждения этого вопроса. У меня есть вопросы от Канады, Нидерландов, Швейцарии и Дании. Канада, пожалуйста.

IAN SHELDON Спасибо, Нико. И спасибо всем докладчикам, это было действительно очень интересно. Я буду краток, потому что знаю, что в зале Zoom большая очередь. Но еще раз спасибо, особенно Грэму, спасибо за отчет NetBeacon. Мне очень понравилась ваша мысль о том, что нельзя позволять прогрессу или стремлению к совершенству стоять на пути прогресса, и мы видим здесь определенный импульс.

И я думаю, что для достижения своевременных результатов очень важно рассматривать узконаправленные, четко определенные PDP. Так что я просто призываю членов GAC ознакомиться с отчетом NetBeacon. Он очень хорошо составлен, это обсуждение политики, он не слишком технический, и в нем есть много действительно хороших предложений. Но еще раз спасибо вам большое, и я с нетерпением жду будущих обсуждений в GAC о том, как мы можем продвигаться вперед с этими PDP. Спасибо.

NICO CABALLERO Спасибо, Канада. Нидерланды.

MARCO HOGEWONING Спасибо. Для протокола, это Марко из Нидерландов. Я присоединяюсь к другим ораторам и благодарю вас за это очень информативное заседание. Я думаю, как только что сказал мой канадский коллега, мы должны учитывать, что идеальное — враг хорошего.

И, как уже упомянула моя коллега из EC, я думаю, что пришло время начать сужать круг вариантов, и я надеюсь, что в следующем напоминании всем нам, вместе с GNSO и Правлением, мы сможем действительно найти какой-то консенсус или одну-две темы для продвижения в период до следующего заседания. Спасибо.

NICO CABALLERO Спасибо, Нидерланды. Швейцария.

JORGE CANCIO Спасибо, Нико. Хорхе Кансио (Jorge Cancio), Швейцария, для протокола. Да, позвольте мне присоединиться к предыдущим ораторам. Я думаю, что важно посмотреть, в каком направлении пойдет обсуждение с GNSO и Правлением. Но я определенно вижу потенциал в идее узконаправленных PDP. И, возможно, небольшое уточнение к оптимистичной оценке Сьюзан. Я не думаю, что когда-либо был PDP, который длился менее года, но я готов признать свою ошибку. Спасибо.

NICO CABALLERO Спасибо вам большое, но будем надеяться, что мы сможем это изменить. Спасибо, Швейцария. Следующая – Дания.

FINN PETERSEN Спасибо, председатель. Финн Петерсен (Finn Petersen) из Дании, для протокола. И спасибо за презентацию, мы ее высоко оценили. Мы согласны с тем, что PDP должны быть узконаправленными, и мы хотели бы увидеть их до начала следующего раунда. Так что это должно быть довольно рано. Мы будем особенно обращать внимание на проактивные меры, я думаю, что массовая регистрация была одной из них.

Мы также хотели бы, чтобы требования к идентификации или проверка контактных данных и так далее были более строгими, чем сегодня. Это то, на что мы будем обращать

внимание. Конечно, есть и другие вещи, транспарентность, но если мы должны расставить приоритеты и что-то сделать до следующего раунда, то, на наш взгляд, следует сосредоточиться на проактивных мерах.

И тогда это будет лишь еще одним шагом на пути к Нирване, или я не знаю, куда мы идем. Один вопрос к Interisle: в вашем исследовании и рассмотрении вы определили, что означает массовая регистрация, где должен быть предел? Должно ли это быть пять регистраций подряд? Спасибо.

GRAEME BUNTON

Очень быстро. Здравствуйте, это Грэм из Института NetBeacon. По поводу повторной массовой регистрации, я думаю, что вы очень быстро столкнетесь с проблемами при попытке определить конкретное ограничение на количество доменов, доступных для покупки в одно и то же время. Злоумышленники сразу же обойдут ограничение и автоматизируют процесс. Это также интересно сказывается на рынке, поскольку, когда домены отображаются в результатах поиска, вы можете добавить один или два в корзину, и количество доменов, доступных в этих результатах поиска, будет зависеть от такого ограничения. Так что теперь мы действительно вмешиваемся в рынок.

И поэтому я считаю, что такой подход рискован. Когда мы думали о том, как решить проблему массовой регистрации, особенно после того, как она была поднята в INFERMAL, мы

пришли к двум выводам. Во-первых, доступ к API, которые позволяют делать подобные вещи, создает препятствия для доступа к инструментам, а не точно определяет, как эти инструменты должны использоваться, и это будет более эффективным способом решения проблемы.

Во-вторых, проверка связанных доменов может помешать проведению кампаний. Таким образом, это хороший реактивный шаг. Но если регистратор обязан проверять все домены в учетной записи клиента, а их может быть 10, 20, 30, 100, то это фактически налог на регистратора, который будет ему стоить денег.

Таким образом, у них будет стимул более тщательно выбирать, кому предоставлять доступ к большому количеству доменов, поскольку теперь они будут обязаны проверять их все. Мы надеемся, и именно поэтому мы включили это в документ, что это окажет влияние на отрасль, будет поощрять правильное поведение, которое мы хотим видеть для решения проблем массовой регистрации. Спасибо.

NICO CABALLERO

Спасибо вам большое. Нам пора заканчивать. Увидеть широкий консенсус в этом вопросе, учитывая международную ситуацию, для нас как благословение. Позвольте мне сказать, что консенсус в наши дни не очень популярен. Так что я вижу широкий консенсус в отношении подхода к рассмотрению вопроса о коммюнике и трех тем, включенных в число важных

вопросов. Я не буду зачитывать все снова, или рекомендации. Но в заключение, Сьюзан, хотели бы вы что-нибудь добавить по этому вопросу, учитывая, что вы являетесь ведущей по теме в PSWG?

SUSAN CHALMERS

Спасибо, господин председатель. Очень кратко, с точки зрения Соединенных Штатов, сроки PDP должны быть значительно сокращены, чтобы достичь успехов в области политики до того, как DNS расширится в результате следующего раунда новых gTLD. Последнее, что я хотела бы сказать, касается более широкого сообщества ICANN. Мы заслушали предложения от NetBeacon, Палата сторон, связанных договорными обязательствами, подготовила предложения.

У Группы коммерческих заинтересованных сторон есть идеи. У Консультативного комитета At-Large есть идеи и приоритеты политики в отношении злоупотреблений DNS. Группа некоммерческих заинтересованных сторон, которая стремится предлагать конструктивные предложения и рекомендации по политике, определила приоритеты политики в отношении злоупотреблений DNS. Но мы все видим, что есть движение, мы движемся в одном направлении, и мультистейкхолдерное сообщество в ICANN должно работать вместе над проблемой злоупотребления DNS, чтобы

добиться результата. Сейчас очень важно, чтобы ICANN выработала политику. Так что спасибо вам большое.

NICO CABALLERO Спасибо вам большое, США. На этом все, на что у нас хватило времени. Только быстро… и извините, что мы затянули, сейчас у нас будет перерыв на кофе на 30 минут. Сразу после этого у нас будет заседание с GNSO, а затем с ALAC, по 45 минут на каждое заседание, а затем перерыв на обед. Большое спасибо. Наслаждайтесь кофе.

[КОНЕЦ СТЕНОГРАММЫ]