ICANN81 | AGM - Обсуждение в GAC борьбы со злоупотреблениями DNS
Вторник, 12 ноября 2024 г. - 10:30 - 12:00 время Турции

DAN GLUCK: Здравствуйте и приветствуем вас на обсуждении в GAC злоупотреблений DNS во вторник, 12 ноября, в 07:30 по Гринвичу. Меня зовут Дэн Глак (Dan Gluck) из Персонала поддержки GAC по вопросам разработки политики ICANN. Пожалуйста, обратите внимание, что это заседание записывается и регулируется Ожидаемыми стандартами поведения ICANN и политикой борьбы с домогательствами в сообществе ICANN. Во время этого заседания вопросы и комментарии будут зачитываться вслух только в том случае, если они будут заданы в чате. 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 Zoom. Пожалуйста, назовите свое имя и язык, на котором вы будете говорить, если это не английский, и не забывайте говорить в разумном темпе. Напоминаю, что столы с микрофонами зарезервированы для членов GAC, наблюдателей и приглашенных гостей. Сейчас я передам слово председателю GAC Нико Кабальеро (Nico Caballero).

NICOLAS CABALLERO: Спасибо вам большое за это. Приветствуем всех на заседании по вопросам борьбы со злоупотреблениями DNS. Для нас большая

честь пригласить ведущих по темам GAC, Мартину Барберо (Martina Barbero) из Европейской комиссии, Оуэна Флетчера (Owen Fletcher) из правительства США и Хаджиме Онга (Hajime Onga) из Японии, надеюсь, я правильно произношу вашу фамилию. Для нас также большая честь пригласить наших докладчиков: Махмута Эсата Йилдирима (Mahmut Esat Yildirim) из Управления ИКТ Турции, Летицию Кастильо (Leticia Castillo) из отдела ICANN по обеспечению выполнения договорных обязательств, Редж Леви (Reg Levy) из Tucows, Денниса Тана (Dennis Tan) из VeriSign и Джеффа Бедсера (Jeff Bedser) из CleanDNS.

Приветствуем всех. Без лишних слов и для экономии времени я передаю слово господину Хаджиме Онга (Hajime Onga) из Японии, который расскажет нам о деталях и нюансах нашей сегодняшней беседы. Пожалуйста, Вам слово.

HAJIME ONGA: Хорошо. Спасибо за это, председатель. Доброе утро всем. Приветствую вас на сегодняшнем заседании. Я - Хаджиме Онга (Hajime Onga), новый представитель GAC от Японии. Это заседание будет проходить под совместным руководством Европейской комиссии, Соединенных Штатов и Японии. И на этом заседании мы приветствуем замечательных гостей из правительства Турции, ICANN, Палаты сторон, связанных договорными обязательствами, CPH и SSAC.

Хорошо. Такова повестка дня на сегодня. После краткого вступления состоится презентация принимающей страны. Далее

отдел ICANN по обеспечению выполнения договорных обязательств проведет брифинг по обновлению информации о злоупотреблениях DNS после реализации поправок к Соглашению об администрировании домена верхнего уровня (RA) и Соглашению об аккредитации регистраторов (RAA) в этом году. Затем мы проведем панельную дискуссию о ситуации после внесения поправок с участием CPH, SSAC и ICANN. Затем мы проведем обсуждение в GAC. Наконец, мы расскажем о следующих шагах на пути к ICANN82 в Сиэтле и обсудим коммюнике.

Во-первых, борьба со злоупотреблениями DNS - одна из главных тем GAC. В Японии эта проблема привлекла широкое внимание - от фишинга в узком смысле, как определено в договорах ICANN, до пиратства манги в более широком смысле. Во-вторых, согласно обновленным RA и RAA, регистратуры и регистраторы gTLD должны рассматривать сообщения о злоупотреблениях DNS в качестве договорного обязательства. В-третьих, в этом договорном соглашении злоупотребления DNS определяются как вредоносное ПО, ботнет, фишинг, фарминг и некоторые случаи спама. В этот раз мы обсудим, какие меры принимаются, в основном в рамках мандата ICANN. А на следующем ICANN мы обсудим усилия всей экосистемы DNS в целом.

Вот общая картина масштабов деятельности ICANN по борьбе со злоупотреблениями DNS. Зеленый квадрат означает, что договорные полномочия ICANN, такие как RA и RAA, ограничены. Это отношения между ICANN и регистратурами, ICANN и регистраторами. Таким образом, такие значимые участники, как

реселлеры, владельцы доменов и ccTLD, не попадают в этот квадрат. Сегодня мы обсудим влияние и эффект отношений в зеленой рамке. На самом деле сообщества заинтересованных лиц, занимающихся проблемой злоупотребления DNS, больше, чем зеленый квадрат.

Во-первых, многие случаи злоупотребления DNS относятся к ccTLD. Проблема злоупотребления DNS широко распространена в отрасли DNS, которая представлена в этом синем прямоугольнике. Кроме того, злоумышленники обычно используют такие услуги, как хостинг-провайдеры и CDN, представленные на этом рисунке красной рамкой. Для борьбы со злоупотреблениями DNS мы должны работать сообща.

В прошлом месяце мы провели вебинар перед конференцией ICANN, и Джефф, который будет участвовать в сегодняшней дискуссии, представил SAC115, который является одной из самых важных ссылок в обновленных RA и RAA. В ходе презентации Джефф представил ряд обсуждений нашей системы борьбы со злоупотреблениями DNS. Он подчеркнул важность сотрудничества между расширенным сообществом DNS. Сегодня на нашем заседании будут рассмотрены пункты, заключенные в красную рамку.

Сначала власти Турции по информационным и коммуникационным технологиям представят свой подход к злоупотреблениям DNS. Как говорится в Кигальском коммюнике ICANN80, изучение конкретных примеров важно для рассмотрения дальнейших мер по борьбе со злоупотреблениями DNS. В этом

выступлении будут представлены турецкие инициативы, включая сотрудничество с администраторами ccTLD и другими соответствующими организациями.

Далее мы обсудим, что можно сделать в рамках ICANN. Во-первых, ICANN проведет брифинг по соблюдению обязательств RA и RAA. Во-вторых, мы проведем панельную дискуссию с заинтересованными сторонами по поводу усилий и влияния поправок. И наконец, мы проведем обсуждение в GAC с учетом этих данных. Затем, на следующей конференции ICANN, мы расширим рамки и обсудим, что можно сделать с расширенным сообществом или экосистемой.

В завершение сегодняшнего заседания мы кратко расскажем о дальнейших шагах для следующей конференции ICANN. Как вы видите, повестка дня на сегодня очень насыщенная. Так что, пожалуйста, уважайте часы, как японцы, но я сегодня не очень хороший учитель, потому что немного выбиваюсь из графика. Извините. В любом случае, давайте перейдем к презентации от принимающей страны, господин Махмут, вам слово.

MAHMUT ESAT YILDIRIM: Спасибо вам большое. Всем привет. Меня зовут Махмут Эсат Йилдирим (Mahmut Esat Yildirim). Я являюсь руководителем отдела Управления информационных коммуникационных технологий Турции. Сегодня я расскажу о механизме борьбы со злоупотреблениями, который мы создаем в турецком

национальном CERT и ccTLD. Я думаю, мы слишком быстро движемся. Хорошо.

NICOLAS CABALLERO: Махмут, будьте добры, говорите ближе к микрофону.

MAHMUT ESAT YILDIRIM: Конечно.

NICOLAS CABALLERO: Спасибо вам большое. Спасибо.

MAHMUT ESAT YILDIRIM: Итак, Турецкий национальный центр CERT и ccTLD Турции находятся в одном ведомстве. Турецкий TR CERT — это Национальный центр реагирования на инциденты кибербезопасности Турции. Его основная задача - выявлять, анализировать и устранять киберугрозы и инциденты по всей стране. И, как я уже говорил, ccTLD, название которого на турецком языке TRABIS, находится в том же департаменте. Вот почему мы можем объединить две власти одновременно для борьбы со злоупотреблениями DNS и другими киберугрозами.

У нас есть Национальные стратегии и планы действий по кибербезопасности. На самом деле, у нас их четыре. И в этих стратегиях и планах действий есть несколько пунктов о злоупотреблениях, которые нужно обнаружить и смягчить, о

механизмах злоупотреблений и о киберугрозах. Последняя версия Национальной стратегии и плана действий по кибербезопасности содержит 4 темы, 6 стратегических задач, 18 целей и 61 пункт действий.

Эти пункты, прежде всего, представляют собой подход к кибербезопасности, ориентированный на человека. Безопасное использование технологий и их вклад в кибербезопасность, киберустойчивость, проактивная киберзащита и сдерживание, внутренние и национальные технологии в борьбе с киберугрозами и, наконец, бренд Турции на международной арене. Все это содержится в нашей Национальной стратегии кибербезопасности и Плане действий.

Наша правовая база для снижения этих киберугроз и злоупотреблений DNS реализуется в соответствии с положениями, изложенными в статьях Закона Турции о коммуникации в ходе выборов, 5809. В статье 60, параграф 11, говорится, что организация принимает или должна принимать все необходимые меры для защиты и сдерживания кибератак на правительственные организации, частные и реальные структуры. Таким образом, этот закон возлагает на Турецкую национальную службу CERT множество обязанностей по сдерживанию и принятию мер против киберугроз.

В следующем пункте того же закона говорится, что организация может получать и оценивать информацию, документы, данные и записи из мест в рамках своих обязанностей. Так что с помощью этого закона мы можем запрашивать данные об информации для

обнаружения кибератак у разных организаций или из разных систем.

Правовая основа ccTLD, особенно в рамках законодательных норм, заключается в том, что ccTLD .tr поддерживает правоохранительные органы в борьбе с киберпреступностью. Мы тесно сотрудничаем со всеми правоохранительными органами, а также с судами, и предоставляем информацию и документы по запросу таких органов, как суды, а иногда мы также тесно сотрудничаем с CERT и правоохранительными органами, чтобы выявлять и пресекать подобные злоупотребления.

Так с какими же видами злоупотреблений мы сталкиваемся почти каждый день? Фишинг, распространение вредоносного ПО, спам, захват доменов, управление ботнетами, иногда материалы об эксплуатации детей, мошенничество и аферы, злоупотребления DNS, технические злоупотребления DNS, такие как подмена DNS или захват DNS, а иногда и нарушение конфиденциальности. Все эти вещи мы пытаемся обнаружить и предотвратить во всех этих категориях, и мы создали некоторые инструменты и механизмы для их обнаружения.

Первый из этих инструментов, которые мы создали, - AZAD, так называемый AZAD. Это программное обеспечение, созданное собственными силами, которое использует механизм искусственного интеллекта, машинное обучение и механизмы искусственного интеллекта, для обнаружения фишинговых доменных имен. Например, мы собираем все новые доменные фиды, а также некоторые другие фиды из разных источников. Мы

собираем миллионы доменных имен каждый день, и с помощью машинного обучения и искусственного интеллекта мы собираем связанные с фишингом доменные имена из этих миллионов доменных имен, так чтобы наши операторы в ccTLD могли вручную проверить, является ли это связанное с фишингом доменное имя действительно фишинговым или это ложное срабатывание.

Так что на данный момент это программное обеспечение успешно работает в 97% случаев. Таким образом, фишинговые адреса, направленные на пользователей в Турции, обнаруживаются и блокируются до или сразу после того, как они становятся активными. Поскольку мы используем возможности CERT, турецкого национального CERT и ccTLD, мы можем тесно сотрудничать с интернет-провайдерами в Турции, так что мы можем действовать очень быстро, чтобы предотвратить эти фишинговые действия. Все эти сообщения, все эти жалобы, связанные со злоупотреблениями, собираются в специальном программном обеспечении, которое мы создали своими силами, — это KULE. Мы собираем все эти уведомления и распределяем их по различным подразделениям.

Вот как работает наш поток злоупотреблений DNS в TRABIS в целом. Мы собираем так много уведомлений из разных источников, таких как владельцы доменов, регистраторы, конечные пользователи или, как я уже говорил, AZAD. Мы собираем все эти уведомления в приложении KULE. Затем мы пересылаем их в TRABIS, который является ccTLD. Затем они анализируют все эти уведомления, используя искусственный

интеллект и все остальное. Затем они могут приостановить действие доменного имени или передать дело интернет-провайдерам.

Таким образом, есть некоторая статистика по реагированию на инциденты с программным обеспечением KULE. Мы собрали более 13 000 жалоб, и из этих 13 000 жалоб 8 000 стали для нас инцидентами. Это означает, что мы должны проверить эти уведомления на предмет того, являются ли они злоупотреблением или нет. Из этих 8 000 5 000 были действительно злоупотреблением, и мы либо отменили домен, либо заблокировали его. На данный момент мы обнаружили более 900 фишинговых сайтов, более 3 400 банковских фишинговых сайтов, 3 центра управления и контроля над вредоносным ПО и 26 имен, выдающих имена вредоносных программ. Все это с помощью созданного нами инструмента искусственного интеллекта.

Есть некоторые общие шаблоны и слова из списка ограниченных имен, например, жалоба. На самом деле, возможно, в английском языке это не имеет смысла, но complaint, implication, dues, cancellation, loan в турецком языке используются для кражи личных данных. А количество слов, содержащих слово banking, не превышает 20, потому что у нас есть ограниченный список доменных имен. Так что мы включили все эти официальные названия банков в список ограниченных доменных имен, чтобы злоумышленные домены или кибер-злоумышленники не могли зарегистрировать доменные имена, связанные с банками.

В турецком языке такие слова, как «возможность», «скидка», «доверие», «онлайн кампания», очень часто используются в фишинговой деятельности или деятельности, связанной со злоупотреблениями. Опять же, возможно, на английском языке для некоторых из вас это не имеет смысла, но мы создаем и совершенствуем наши механизмы искусственного интеллекта, расширяя эти виды слов. И каждый день мы учим новые механизмы и новые слова, чтобы улучшить механизм искусственного интеллекта для обнаружения злоупотреблений.

TRABIS был создан в 2022 году, а после 2022 года произошли некоторые поворотные моменты. До TRABIS все регистрации доменов осуществлялись на основе документов для com.tr, net.tr или org.tr. Вы должны были предоставить официальный документ. Но после TRABIS все будет происходить в порядке живой очереди. Вот почему участились случаи злоупотреблений. Поэтому мы должны улучшить наши механизмы обнаружения. Кроме того, после 2023 года мы начнем использовать возможности CERT вместе с TRABIS, так что мы сможем быстрее их устранять.

Наши методы подачи жалоб — это может быть электронная почта из методов подачи жалоб CERT, веб-страница или горячая линия. Они могут просто позвонить нам и рассказать о любых злоупотреблениях. Так что, если вы зайдете на сайт usom.gov.tr, то увидите адреса, внесенные в черный список. Он находится в открытом доступе для всех. Мы делимся этим списком со всем миром, так чтобы вы могли реализовать эти черные списки доменных имен или IP-адресов, доменных имен вредоносных

программ или фишинговых доменных имен в своих собственных проектах, в своих файерволах или в других черных списках.

Так что мы открыты к сотрудничеству с членами GAC и поиску наиболее эффективных мер по борьбе со злоупотреблениями DNS. И нам интересно узнать о политике злоупотреблений в других ccTLD и других странах, о том, как они их выявляют и как борются с ними. Мы можем обмениваться опытом и хотели бы поделиться своим опытом, как мы реализуем эти политики или эти механизмы в наших процессах. И если у вас есть вопросы, не стесняйтесь их задавать. Спасибо вам большое.

NICOLAS CABALLERO: Большое спасибо за это, Махмут. Итак, на данный момент можно задавать вопросы Махмуту. Я пока не вижу ни одной поднятой руки. У меня есть несколько вопросов, касающихся методов, которые вы используете для выявления аномалий в DNS-трафике, DNS-запросах и спаме в целом.

С вашей точки зрения или согласно вашему опыту, какие методы искусственного интеллекта являются наиболее успешными для таких случаев, например, не знаю, random forest (Метод случайного леса) или глубокое обучение? И в таком случае, что за глубокое обучение? Нейронные сети, конволюционные нейронные сети или вообще? Я не хочу слишком углубляться, но просто хочу иметь представление о том, что лучше всего работает с вашей точки зрения и согласно вашему опыту.

MAHMUT ESAT YILDIRIM: Это действительно хороший вопрос. И вообще, мне нравится техническая сторона этого вопроса. В процессе машинного обучения есть две разные стороны. Во-первых, мы используем методы машинного обучения для обнаружения вновь зарегистрированных доменных имен, чтобы проверить их сходство. Например, я зарегистрировал домен mahmut.com, и наши модели машинного обучения проверяют, является ли он на 90% фишинговым сайтом или нет, как мы учили раньше.

NICO CABALLERO: Random forest.

MAHMUT ESAT YILDIRIM: Да, в целом. Но, с другой стороны, мы тесно сотрудничаем с интернет-провайдерами, с CERT, они используют свои собственные сетевые системы, интернет-провайдеров, огромные сетевые системы для обнаружения других видов злоупотреблений DNS, таких как перехват DNS или сетевые атаки, связанные с техникой DNS. Они также используют различные методы машинного обучения для обнаружения перетекающих пакетов. И они сообщают нам об этом. Когда интернет-провайдеры обнаруживают такую атаку, они сообщают нам. Затем вместе с экспертами ccTLD и экспертами CERT мы принимаем меры по реагированию на инциденты, чтобы обнаружить и устранить последствия этих атак.

NICOLAS CABALLERO: Спасибо. Спасибо вам большое за это. У меня Европейская комиссия, а затем Мустафизур. Европейская комиссия, Вам слово.

GEMMA CAROLILLO: Большое спасибо, Нико. Гемма Каролилло (Gemma Carolillo) из Европейской комиссии. Спасибо турецкому коллеге за очень интересную презентацию. У меня есть пара вопросов, потому что в Европейском союзе для нашего собственного ccTLD .eu мы также используем очень похожий подход. Они используют искусственный интеллект и машинное обучение на этапе предотвращения, так что в основном предотвращают регистрацию вредоносных доменных имен.

Но ваш подход, похоже, идет еще дальше. Он кажется более интересным, потому что, насколько я понимаю, вы интегрируете данные об угрозах из CERT и, следовательно, способны перейти не только к фазе предотвращения, но и к обнаружению и даже реагированию, если я правильно поняла. Так что, если бы вы могли это уточнить.

И потом, я не знаю, есть ли у вас информация, можете ли вы поделиться ею, потому что мы много обсуждали эти инструменты в этой группе. Вы говорите, что они разрабатываются собственными силами ccTLD. Если у вас есть информация о стоимости такой системы и как вы думаете, будут ли эти системы

открытыми, можно ли их легко использовать, легко интегрировать в другие регистратуры. Спасибо.

MAHMUT ESAT YILDIRIM: Спасибо вам большое. Наши механизмы CERT, как правило, используют наших собственных разработчиков, наши собственные исследования и разработки внутри компании. На создание этого механизма ушел почти год. На самом деле, это могло бы занять меньше времени, но, возможно, больше года ушло на обучение алгоритмов машинного обучения для создания новых моделей. До появления этих алгоритмов, до создания программного обеспечения у нас было несколько операторов, работавших вручную. Вручную они помечали доменные имена как фишинговые, вредоносные или другие типы. Поэтому у нас есть огромный список доменов с метками. С помощью этого списка доменов мы обучаем, создаем новые модели и совершенствуем их каждый день. Вот почему он действительно успешен.

С другой стороны, с помощью механизма CERT мы можем, как вы уже сказали, напрямую предотвратить злоупотребления. CcTLD может обнаружить злоупотребления, или кто-то может уведомить CcTLD, что есть фишинговый сайт, или они могут обнаружить его. И с помощью CERT, в сотрудничестве с интернет-провайдерами, в течение, возможно, пяти минут, мы можем заблокировать доступ к этому доменному имени. Мы также можем аннулировать домен, мы можем его захватить, или мы можем напрямую заблокировать его. Это зависит от конкретного случая. Если речь идет о

командовании и управлении вредоносным ПО, мы напрямую блокируем его на уровне интернет-провайдера. Спасибо.

NICOLAS CABALLERO: Спасибо вам большое за это, Махмут. У меня есть еще два вопроса. Мы не станем мучить Махмута тысячей вопросов. У меня самого есть много других. У меня Бангладеш, а затем Индия. Пожалуйста, будьте краткими и переходите сразу к делу. Вам слово, пожалуйста.

MUSTAFIZUR RAHMAN: Большое спасибо, господин Махмут, за прекрасную презентацию. Как вы сказали в своей презентации, после проверки документов количество жалоб сократилось. Мой вопрос заключается в том, что проверка документов требует времени, но, с другой стороны, клиенту нужно быстрое обслуживание. Как вы балансируете эту проблему? Спасибо.

MAHMUT ESAT YILDIRIM: На самом деле, это было до появления TRABIS. До 2022 года, как вы уже сказали, это был очень медленный процесс. Вы могли попытаться зарегистрировать доменное имя com.tr и подать официальные документы, возможно, на четырех или пяти страницах, затем операторы должны были проверить, действительны ли эти документы или это мошенничество, используя различные механизмы, после чего они могли выдать вам доменные имена. Но теперь, после 2022 года, все не так.

Теперь все происходит по принципу «первый пришел - первый обслужен». Мы не требуем никаких документов.

NICOLAS CABALLERO: Спасибо вам за это. И тут где-то звонит телефон. У меня на очереди Индия. Вам слово.

T. SANTHOSH: Спасибо, председатель. Для протокола говорит Т. Сантош. И спасибо, Махмут, за презентацию. Мой вопрос заключается в том, открыт ли домен .tr для всего мира? Если да, то какую проверку вы проводите для них? Спасибо.

MAHMUT ESAT YILDIRIM: Домен .tr открыт для всех желающих, но в Турции есть несколько разрешенных регистраторов. Так что вы можете использовать только этих регистраторов для регистрации доменного имени .tr. При этом вы должны иметь корректные данные WHOIS и предоставлять корректные данные WHOIS, например, адрес электронной почты или физический адрес, а также номера телефонов. Это похоже на .com или некоторые другие gTLD.

NICOLAS CABALLERO: У меня есть последний вопрос. Это единственный шанс задать его вам. Так что я должен это сделать, извините. Прежде чем я передам слово Оуэну из США. Что лучше работает для DNS-туннелирования, согласно вашему опыту, например,

многослойный перцептрон с точки зрения нейронных сетей или наивный Байес? Что сработало лучше в вашем случае?

MAHMUT ESAT YILDIRIM: На самом деле, в этом контексте я думаю, что использование данных о потоках и нейронных сетей может быть лучше. Потому что мы не можем быть уверены в том, как они используют, как реализуют эти механизмы туннелирования DNS. Мы не можем быть уверены в том, что они проталкивают через эти туннели. Так что, возможно, мы можем собирать пакеты. Возможно, мы соберем пакеты и с помощью нейронных сетей научим их обнаруживать DNS-туннелирование в огромном количестве пакетов, а затем сможем детально проанализировать их вручную.

NICOLAS CABALLERO: Большое спасибо. У меня Бангладеш, а затем я предоставлю слово США. Бангладеш, пожалуйста, Вам слово. Простите, извините, это была старая рука. Я перейду к... Простите. Я видел руку. Это Ливия? Ливия? Вам слово, пожалуйста.

KHALED ALTARHUNI: Спасибо, председатель. Вопрос к Махмуту. Спасибо, Махмут, за хорошую презентацию. Я хотел бы узнать, работает ли система с легальным контентом в домене, таким как текст, изображения? Спасибо.

MAHMUT ESAT YILDIRIM: Да, на самом деле, это программное обеспечение, которое мы создали, AZAD, я не упоминал подробно, но оно проверяет сходство доменного имени, а также контекст этого сайта. Сначала он подает сигнал тревоги, когда обнаруживает, что это фишинг, например, 95 %, и подает сигнал тревоги. Но на этом сайте нет контекста, так что мы ничего не можем с этим сделать. Например, если человек держит в руках пистолет, это не значит, что он собирается в кого-то стрелять.

Поэтому мы должны увидеть, что на этом сайте есть злоупотребления. И алгоритм машинного обучения проверяет контекст веб-страницы, обновляется ли она, а затем, когда мы видим реальную неправомерную активность в контексте, например фишинговый сайт или другие виды, мы принимаем меры и предотвращаем ее. Спасибо.

NICOLAS CABALLERO: Большое спасибо, Махмут. Действительно. Спасибо, Ливия, за вопрос. В этот момент позвольте мне передать слово Оуэну Флетчеру (Owen Fletcher) из правительства США. Извините, что заставил вас ждать. Вам слово.

OWEN FLETCHER: Спасибо. Здравствуйте, это Оуэн Флетчер (Owen Fletcher) из Соединенных Штатов. Я думаю, что мы немного отстаем от графика нашего заседания, так что я буду очень краток. И я думаю, что все наши докладчики на оставшейся части заседания также

знают, мы постараемся быть быстрыми. Но у нас здесь Летиция Кастильо (Leticia Castillo) из отдела ICANN по обеспечению выполнения договорных обязательств, чтобы представить нам обновленную информацию о поправках к договору о злоупотреблениях DNS, которые GAC приветствовал ранее в этом году, и GAC выразил заинтересованность в отслеживании их воздействия и правоприменения. Так что я передаю слово Летиции. Спасибо.

LETICIA CASTILLO: Спасибо, Оуэн. Всем привет. Меня зовут Летиция Кастильо (Leticia Castillo). Я являюсь старшим директором отдела ICANN по обеспечению выполнения договорных обязательств. Как сказал Оуэн, я собираюсь представить обновленную информацию о первых шести месяцах применения новых требований по злоупотреблениям DNS, которые вступили в силу 5 апреля. Я также хочу подчеркнуть, что на прошлой неделе, 8 ноября, мы опубликовали подробный отчет о первых шести месяцах обеспечения соблюдения требований. Он состоит из 17 страниц и содержит множество информации о проведенных расследованиях, результатах, примерах ответов и действий, которые были признаны соответствующими требованиям. Так что ознакомьтесь с отчетом, если хотите получить еще больше информации о предпринятых правоприменительных мерах.

А теперь перейдем к данным. С 5 апреля 2024 года по 5 октября 2024 года мы инициировали 192 расследования злоупотреблений DNS в отношении регистраторов и регистратур. Это были дела,

связанные как минимум с одним видом злоупотребления DNS, под которым в соглашениях ICANN понимаются фишинг, фарминг, вредоносное ПО, ботнеты и спам, когда спам специально используется для доставки одной или нескольких других четырех форм злоупотребления DNS. В результате этих расследований в двух случаях оператору регистратуры и регистратору было направлено официальное уведомление о нарушении за несоблюдение требований к злоупотреблениям DNS.

154 расследования злоупотребления DNS были урегулированы нами на так называемом этапе неформального урегулирования — это процесс, в ходе которого мы разрешаем большинство жалоб всех типов, поскольку регистратор или регистратура демонстрируют соответствие требованиям или принимают меры по устранению несоответствия до того, как будут предприняты дополнительные меры по соблюдению требований.

И поскольку одно дело может касаться как одного доменного имени, так и нескольких, и поскольку одно расследование, касающееся нескольких доменных имен, может привести к обнаружению дополнительных злоумышленных доменов в учетной записи, например, эти 154 расследования привели к приостановке более 2 700 вредоносных доменных имен и отключению более 350 веб-сайтов в этих случаях, поскольку регистратор или реселлер также выступал в качестве хостинг-провайдера для этих доменных имен.

Я также хочу отметить, что это цифры за период, первые шесть месяцев, с 5 апреля по 5 октября. В настоящее время мы ведем

несколько расследований, сотни доменных имен, часть из них, другие были закрыты после 5 октября, так что они не учитываются при расследовании, но будут включены в будущие обновления.

В течение этих шести месяцев мы также принимали участие в многочисленных мероприятиях, направленных на повышение осведомленности сообщества о новых требованиях. Например, в сентябре мы участвовали в семинаре со сторонами, связанными договорными обязательствами, в Пекине, где особое внимание было уделено новым требованиям к злоупотреблениям DNS. То же самое было в Стамбуле в прошлом месяце. Мы тесно сотрудничаем с нашими коллегами из GDS и GSC, которые проводят подобные мероприятия по наращиванию потенциала в рамках многогранной программы ICANN по борьбе со злоупотреблениями DNS.

Мы только что запустили аудит, направленный на проверку соблюдения соглашения об администрировании домена верхнего уровня, включая требования по злоупотреблениям DNS, не ограничиваясь ими, но включая их. В июне мы начали публиковать ежемесячные отчеты о соблюдении требований по злоупотреблениям DNS. Эти отчеты разбиты по типам злоупотреблений DNS и соответствующим правоприменительным мерам.

Они начинаются с данных за апрель 2024 года и обновляются каждый месяц. Формат, который мы использовали для этих отчетов, действительно дает полное представление об этих случаях, если дополнить его регулярными обновлениями с

выводами и результатами, такими как те, которые мы представляли ранее, и отчет от 8 ноября, но мы всегда намеревались продолжать развивать эти отчеты и улучшать их со временем. Поэтому мы приветствуем отзывы сообщества. Я уже упоминала об отчете от 8 ноября. Ссылка на него также находится внизу этого слайда.

Ранее я упоминала о 154 случаях злоупотребления DNS, которые мы разрешили. На этом слайде представлено краткое описание причин, по которым они были разрешены. Что касается дел с регистраторами, то их число составляет 151. Примерно в 52 % случаев регистратор подтвердил факт злоупотребления DNS и принял меры по его пресечению, приостановив действие доменных имен. Приблизительно в 21 % случаев регистратор не обнаружил никаких действенных доказательств злоупотребления DNS, и его ответ был признан соответствующим требованиям, поскольку он предоставил нам разумное объяснение того, что было сделано для расследования и как он пришел к такому выводу.

Например, регистратор проанализировал всю имеющуюся у него информацию и доказательства, касающиеся доменного имени, включая информацию об учетной записи, включая обмен информацией с владельцем домена и владельцем учетной записи, и определил, что владелец домена действительно действовал с ведома и согласия организации, которая, как считается, выдавала себя за него, чтобы провести имитацию фишинговой программы с использованием доменного имени. Это один из примеров.

Примерно в 12 % случаев регистратор принимал меры, чтобы пресечь злоупотребление DNS, например, направлял претензию владельцу домена, который затем принимал меры по отключению URL-адреса, на котором было размещено злоупотребление DNS. Примерно в 3 % случаев регистратор предпринимал другие действия для прекращения злоупотребления DNS. Например, синхронизировал вызовы или перенаправлял серверы имен так, что пользователи, пытавшиеся обратиться к вредоносному доменному имени, перенаправлялись на IP-адреса, контролируемые регистратором. Это касается регистратора.

Давайте поговорим о регистратурах. Мы разрешили три случая злоупотребления DNS с операторами регистратуры, и во всех случаях все доменные имена были приостановлены регистратурой. Опять же, это были резолверы. Многие другие находятся в процессе. У нас также было одно дело, которое ограничивалось проблемами с контактом злоупотребления. Они также были решены. Разница в количестве дел, решенных с регистраторами и регистратурами, согласуется с тем фактом, что из всех полученных жалоб 94 % были направлены регистраторам. Из всех начатых расследований 97 % были направлены регистраторам, остальные - регистратурам.

Но у нас нет ни минимума, ни максимума для начала расследования или передачи на более высокий уровень. Доказательством этого является то, что за тот же период мы направили публичное официальное уведомление о нарушении регистратуре и публичное уведомление о нарушении

регистратору. Как я уже говорила, это цифры за первые шесть месяцев. У нас многое происходит. Многое было решено после 5 октября, и мы намерены продолжать предоставлять обновления и выпускать отчеты о неразрешенных проблемах. Я хочу остановиться на этом, чтобы у нас было время ответить на вопросы.

OWEN FLETCHER: Спасибо. Я нашел эту информацию очень полезной, и я полагаю, что все остальные тоже. Я считаю, что эта тема важна для GAC. Я уверен, что у нас есть вопросы от аудитории. Нико, вы хотели бы?

NICOLAS CABALLERO: Да, у нас есть время для нескольких вопросов. У меня Индия.

T. SANTOSH: Спасибо, председатель. Для протокола говорит Сантош. В этой презентации было довольно кратко рассказано о роли регистратур и регистраторов. Из Индии за этот период мы подали три таких жалобы через этот сайт договорных жалоб, но дело в том, что у нас нет никакого статуса этих жалоб. Не поступает она и на нашу почту. Так что, каков статус жалобы, которую мы подали? Она не отражается. Можете ли вы объяснить это? Спасибо.

LETICIA CASTILLO: Здравствуйте, это Летиция Кастильо (Leticia Castillo). Спасибо за ваш вопрос. Если я правильно поняла, вы подали три жалобы, как

вы, кажется, указали, и не получили обновленной информации о статусе выполнения. Я полагаю, что мне известно о жалобах, на которые вы ссылаетесь, и я полагаю, что мы запросили определенную информацию и попросили предоставить дополнительное время для ее предоставления, и мы ждем их.

Но я, конечно, могу просмотреть их вместе с вами в режиме офлайн, чтобы убедиться, что я имею в виду именно те жалобы. Но это часть процесса, когда подается жалоба, приходит подтверждение, в котором указывается идентификатор дела, а затем процессор рассылает заявителю дополнительные сообщения с запросом дополнительной информации. Такое случается часто. Мы проводим всестороннее рассмотрение каждой жалобы.

Во многих случаях нам требуются разъяснения, дополнительные доказательства от заявителя, и мы отправляем, что получаем их, такие случаи, как в примере, несколько раз, а также получаем запросы от наших заявителей на дополнительное время, так чтобы они могли собрать информацию, которую мы запрашиваем, и предоставить ее нам. А когда дела решены, они также получают объяснение, почему дело решено, и как связаться с отделом по обеспечению выполнения договорных обязательств, если у них возникнут вопросы по поводу решенного дела. Это также рассылается вместе с каждым отправленным нами сообщением. Я буду рада пообщаться с вами в офлайн-режиме и предоставить вам дальнейшую информацию об этих жалобах.

NICOLAS CABALLERO: Спасибо вам большое за это. У меня Нидерланды, а затем США. Пожалуйста, постарайтесь быть краткими. Вам слово.

ALISA HEAVER: Спасибо. Это Алиса Хивер (Alisa Heaver) для протокола. Спасибо за презентацию. Мне хотелось бы узнать, в какой степени эти цифры или как эти цифры сравниваются с цифрами полугодовой или годовой давности, когда новые меры еще не были введены? И мой второй вопрос: какова средняя продолжительность расследования, прежде чем регистратор примет меры? И в какой степени расследования, которые были начаты, основаны на новых договорных мерах? То есть, дополнениях к предыдущему своду правил. Спасибо.

LETICIA CASTILLO: Спасибо за вопрос. Итак, что касается цифр, то за последние несколько лет, даже до 5 апреля, мы наблюдаем рост числа жалоб, которые мы получаем в связи со злоупотреблениями. Просто приведу данные. В 2023 году мы получали в среднем более 1300 новых жалоб в месяц, которые добавлялись к уже существующим делам. С января по сентябрь 2024 года в среднем поступало почти 2 000 новых жалоб в месяц. Таким образом, рост точно есть, причем еще до апреля 2024 года.

Что касается времени, которое занимает расследование, то оно полностью зависит от типа расследования. У нас есть дела о злоупотреблениях DNS с одним доменным именем. Все очень

просто. Мы связываемся с регистратором. Регистратор отвечает согласием. Доменное имя должно быть удалено. Оно удаляется.

Это может быть сделано в течение одного дня. У нас есть расследование, включающее тысячи доменных имен, в ходе которого договорной стороне направляется запрос не только на рассмотрение отчета о злоупотреблениях, но и на выявление закономерностей, указывающих на отсутствие у них процесса устранения злоупотреблений DNS. Так что дело не только в этом отчете. Это влияет на будущие отчеты и на то, как они в целом решают проблему злоупотребления DNS.

Мы запрашиваем у них план исправления ситуации, а также информацию о том, как они собираются его реализовать, этапы и сроки реализации, чтобы убедиться, что они внедрили этот процесс. И мы ждем, пока этот процесс не будет внедрен, тестируем его, а затем закрываем и отслеживаем, потому что если после его реализации возникают повторные проблемы, то принимаются меры по передаче решения жалобы на более высокий уровень. Все зависит от конкретного случая, сколько времени это займет.

NICOLAS CABALLERO: Большое спасибо. У меня есть еще один запрос на слово, США. Лорин, Вам слово, пожалуйста.

LAUREEN KAPIN: Да, это Лорин Капин (Laureen Kapin), я говорю в качестве члена Рабочей группы по обеспечению общественной безопасности. Я хотела выразить благодарность за проделанную здесь работу и сказать, что очень радует то, что мы видим эти конкретные меры по борьбе со злоупотреблениями DNS, и это знак того, что это нужные эффективные изменения. Мой вопрос заключается в том, что здесь, на слайде, есть категория. Регистратор принял меры по пресечению злоупотребления DNS, что является отдельной мерой, помимо приостановки действия доменного имени. Можете ли вы рассказать о том, какие виды нарушений вы наблюдаете?

LETICIA CASTILLO: Спасибо, Лорин. Обязательство по соглашению заключается в принятии мер по прекращению или пресечению злоупотребления DNS, а конкретные действия будут зависеть от конкретных обстоятельств дела. Как правило, явный случай злоупотребления DNS доменным именем, которое было зарегистрировано для совершения этого злоупотребления, обычно приводит к приостановке действия доменного имени. Существуют и другие случаи, подобные тому, который я приводила в качестве примера.

Например, в данном конкретном случае, о котором я думаю, это было взломанное доменное имя, и регистратор связался с владельцем домена и сообщил, что это происходит. Вам нужно сделать все необходимые действия, чтобы убедиться, что этого больше не произойдет. Регистратор пошел дальше и позаботился о самом URL. Это было нарушение со стороны регистратора, и оно было признано соответствующим соглашению.

NICOLAS CABALLERO: Большое спасибо. Я снова передаю слово Оуэну.

OWEN FLETCHER: Спасибо, Нико. Это Оуэн Флетчер (Owen Fletcher). Я согласен с тем, что это замечательно, что публикуются метрики, связанные с обеспечением соблюдения поправок к договорам, и замечательно видеть результаты, о которых вы уже сообщаете. Мы переходим к групповой дискуссии, а слайды будут подняты. В ней участвуют Редж Леви (Reg Levy) из Tucows, Деннис Тан (Dennis Tan) из VeriSign и Джефф Бедсер (Jeff Bedser) из CleanDNS, а также SSAC. Они ответят на несколько вопросов на следующем слайде, пожалуйста.

Один из вопросов адресован только Редж и Деннису, поскольку в нем говорится, что вы, как договорная сторона, сделали после внесения поправок? Пожалуйста, помогите нам это понять. Второй и третий вопросы предназначены для всех. Каковы, по вашему мнению, влияние и последствия поправок? И какие уроки были извлечены из первых шести месяцев реализации поправок? Это поможет нам узнать больше мнений и продолжить изучение последующих действий в связи с поправками. Мы стараемся уложиться в три минуты для каждого из вас. Извините, если я вас прерву, если вы превысите отведенное время, но я постараюсь, чтобы мы придерживались определенного графика. И мы можем начать с Редж?

REG LEVY: Спасибо, Оуэн. Редж Леви (Reg Levy) из компании Tucows, регистратора доменных имен. Tucows принимала самое непосредственное участие в переговорах по поправкам. Так что многое, ну, главное, что я хочу сказать, — это то, что мы мало что изменили после принятия поправок, потому что мы считаем, что изначально все делали правильно. Но мы очень рады, что поправки теперь являются частью наших договорных обязательств. У меня есть команда из семи специалистов по борьбе со злоупотреблениями DNS, которые рассматривают все поступающие сообщения, чтобы подтвердить факт предполагаемого злоупотребления и принять меры по его устранению.

Одна из вещей, которую мы начали делать, и которая изменилась после принятия поправок, хотя, возможно, и не из-за поправок, заключается в том, что мы начали не приостанавливать работу многих фишинговых доменов, а перенаправлять их (sinkholing). Синкхолинг означает, что мы направляем NS-записи домена на определенный набор DNS-серверов, которые фактически управляются CleanDNS здесь, на панели, так что они могут получить дополнительную информацию о фишинговых кампаниях и увидеть тенденции среди регистраторов. Мы можем видеть определенные вещи, которые происходят в нашем пространстве имен, но такая группа, как CleanDNS, может видеть более широкие тенденции в отрасли. И мы надеемся, что эта информация, которую мы им предоставляем, поможет им лучше выявлять кампании в отрасли.

OWEN FLETCHER: Спасибо, Редж. Это было меньше трех минут. Отличная работа. Деннис, не хотите ли вы выступить следующим?

DENNIS TAN: Спасибо, Оуэн. Мне нечего добавить к сказанному Редж в отношении влияния поправок о злоупотреблениях DNS. Что касается операторов регистратуры, то большая часть ответственности лежит на регистраторах, которые напрямую взаимодействуют с владельцами доменов. На уровне регистратуры мы обычно рассматриваем масштабные угрозы безопасности, такие как, например, ботнет DGA, и именно здесь операторы регистратуры способны предотвратить регистрацию таких доменных имен, поскольку они подвергаются обратной разработке и не имеют конкретного списка доменных имен, которые могут быть использованы на уровне регистратуры.

В отношении зарегистрированных доменных имен мы, скорее всего, передадим их регистратору, так что он будет работать с владельцами доменов наиболее подходящим способом, чтобы смягчить или пресечь злоупотребления DNS. Думаю, я просто хочу сказать, что в целом, и я говорю от имени всех операторов регистратуры, одним из аспектов, которому поправки о злоупотреблениях способствовали с практической точки зрения, является повышение уровня качества отчетов о злоупотреблениях. Теперь, когда сообщения о злоупотреблениях требуют доказательств, это облегчает нам оценку и определение,

проверку того, в чем заключается злоупотребление, и принятие соответствующих мер в этой связи.

Я также хочу отметить то, что обе наши группы, объединенная CPH, рабочая группа по борьбе со злоупотреблениями DNS, делали с момента принятия поправок по борьбе со злоупотреблениями DNS, о которых мы всегда говорили, что это будет первым шагом в многочисленных мероприятиях по борьбе со злоупотреблениями DNS. Мы работаем и проводим разъяснительную работу с другими группами сообщества ICANN, чтобы найти общие проблемы, над которыми мы можем работать, будь то работа над политикой или просто поиск лучших практик или поиск решений этих проблем.

Совсем недавно, и, возможно, некоторые из вас присутствовали на заседании в начале недели с NCSG, сотрудником CPH, где рассматривались методы борьбы со злоупотреблениями DNS через призму оценки воздействия на права человека. Это один из примеров нашей работы с сообществом ICANN. Думаю, я сделаю паузу, да, в интересах времени, и снова обращусь к вам, Оуэн.

OWEN FLETCHER: Спасибо, Деннис. Замечательно. Джефф, давайте перейдем к вам. У вас есть несколько слайдов, так что.

JEFF BEDSER: Спасибо. Я пропущу первые несколько слайдов, потому что они повторяют то, что уже было представлено. Хорошо. Я хочу сравнить данные. Прошу прощения. Я всю неделю пытаюсь

сохранить голос. Я постараюсь говорить так, чтобы вы меня хорошо понимали. Я хочу поделиться некоторыми данными, которые касаются более широких объемов, злоупотребления DNS. Мы хотим представить в перспективе те объемы, о которых мы говорим.

За период с апреля по июнь мы обработали около 628 000 сообщений о злоупотреблениях. Это примерно 160 000 уникальных доменов. Множество сообщений приходится на меньшее количество доменов. Среднемесячный объем до поправок в отношении обязательств составлял около 225 000 сообщений в месяц. А после изменения в обязательствах он немного увеличился и составил в среднем около 240 000 отчетов в месяц.

В разговорах с регистраторами, регистратурами и некоторыми хостинговыми компаниями они отметили это увеличение. Я думаю, это происходит из-за того, что они знают об изменении обязательств, и многие составители отчетов начали генерировать больше отчетов. Хотя один составитель отчета может сообщить об одном и том же домене хостинговой компании, регистратору и регистратуре, таким образом, на один инцидент может приходиться три отчета.

Так что вот вам пример ежемесячного объема отчетов о фишинге с сентября 2024 года по октябрь 2023 года. Вы можете видеть, что в среднем за месяц объемы составителей отчетов периодически скачут, а иногда и падают. Но в основном объем составителей

отчетов остается примерно одинаковым для всех фишинговых атак.

Это показалось мне очень интересным. Регистратура, которая подверглась взлому, - это публичный отчет ICANN о взломе - была .top. И мы посмотрели на дату, месяц уведомления о взломе - июль. В том месяце было получено в общей сложности около 7 000 отчетов о злоупотреблениях в домене .top. В августе объем был немного выше, чуть меньше 8 000. В сентябре объем снова увеличился еще на 2 000. А в октябре - уже 13 000. Это отличный пример того, как отдел ICANN по обеспечению выполнения договорных обязательств выбрал очень удачную кандидатуру для нарушения в этом вопросе.

Потому что, очевидно, несмотря на уведомление о нарушении и продление, количество отчетов о злоупотреблениях в этой зоне продолжает расти. Так что это не говорит о том, что отдел ICANN по обеспечению выполнения договорных обязательств не справился со своей работой. Это отличный пример того, что они выполняют свою работу. Это тот тип участников, на которых было направлено изменение обязательств - участников, которые не устраняли злоупотребления. И такие объемы, как этот, свидетельствуют об этом.

Сейчас мы измеряем, конечно, общее количество обработанных отчетов, общее количество задействованных доменов. И в среднем это может быть соотношение 3 к 1, 2 к 1, количество сообщений к количеству доменов, количество действий, предпринятых отделом ICANN по обеспечению выполнения

договорных обязательств в отношении регистратора, и, конечно, количество уведомлений о нарушениях. На следующем слайде я хотел бы предложить, что мы должны измерять, потому что гораздо важнее понять, как обязательства меняют поведение и тем самым изменяют масштабы виктимизации в результате злоупотребления DNS.

Сколько отчетов получили достаточные доказательства для принятия мер? Потому что количество отчетов — это прекрасно, но, будучи компанией, которая обрабатывает около 8 миллионов отчетов в год, я могу сказать, что примерно половина из них не имеет достаточных доказательств для принятия каких-либо мер. Они ошибочны, классифицированы неправильно. Вред был устранен до того, как о нем сообщили.

Так что, благодаря новому стандарту доказательств, очень полезно знать, сколько сообщений действительно передаются сторонам, которые соответствуют стандартам, необходимым для принятия мер. Как долго длился вред? Это то, что меня очень волнует, потому что чем короче жизненный цикл домена, используемого для злоупотреблений, тем меньше жертв. В настоящее время этот показатель составляет около 48 часов. Я думаю, что, используя технологии искусственного интеллекта и машинного обучения, мы определенно можем добиться двух минут в этих процессах. Так что о злоупотреблении сообщается, оно подтверждается и устраняется.

Следующая точка измерения, и я знаю, что это еще одна часть ICANN с метрикой домена, и офис OCTO работает над этим, -

насколько эффективными были меры по снижению общего объема? Потому что сейчас, конечно, американский термин — это «уакамоле» («whack-a-mole»). Убираешь один, на его место приходит другой, еще 100. Но когда мы достигнем эффективной точки, когда будет устранено достаточное количество нарушений, будет проведена достаточная работа по снижению воздействия, и мы начнем видеть изменения в поведении злоумышленников. И наконец, сколько усилий нужно приложить, чтобы заставить не соответствующую требованиям сторону выполнять требования по борьбе со злоупотреблениями? Я оставлю этот вопрос на усмотрение отделов ICANN по обеспечению выполнения договорных обязательств.

OWEN FLETCHER: Джефф, простите, что прерываю вас. Мы превысили время. Вы можете закончить? Спасибо.

JEFF BEDSER: Это мой последний слайд. Но я очень быстро подведу итог: я думаю, что изменения в отношении обязательств были хорошими. Я думаю, что изменения в поведении всех сторон - сторон, сообщающих о вреде, - значительно возросли. Я думаю, что продолжаю наблюдать за развитием этих тенденций. Я вижу, что стороны, которые являются проблемой, то есть стороны, которые находятся вне экосистемы и не предпринимают действий, становятся заметными из-за того, что не предпринимают этих действий. И я думаю, что это более важная история, которую

можно рассказать, хорошо это или плохо, — это то, как поправки оказывают систематическое воздействие. И я думаю, что шесть месяцев, прошедших с момента принятия поправок, являются хорошим признаком того, что дела идут в правильном направлении.

OWEN FLETCHER: Спасибо, Джефф. У нас также есть краткое заявление от представителя ICANN по глобальным доменам и стратегии, Мукеша Чулани (Mukesh Chulani). Мукеш, вы можете выступить следующим. Спасибо.

MUKESH CHULANI: Да, спасибо, Оуэн. Я просто хотел подчеркнуть нашу уверенность в том, что мы видим влияние поправок на уровне конкретных дел. Мы работаем уже шесть-семь месяцев, и вы слышали от сторон, связанных договорными обязательствами, мы видели некоторые сводные отчеты от отдела по обеспечению выполнения договорных обязательств. Вы также видели, что сторонний специалист по метрикам отмечает положительное влияние.

Здесь есть определенный импульс. Поправки о злоупотреблениях, как уже упоминал Деннис, никогда не должны были стать окончательным шагом вперед. Это первый шаг вперед. И можно ожидать, что предпочтения будут меняться, можно ожидать, что векторы атак будут меняться. Так что мы должны продолжать следить за этим, следить за дискуссиями.

С нашей точки зрения, отдел по контролю исполнения договорных обязательств занимается обеспечением соблюдения договорных обязательств. У нас есть данные по договорам, очень ориентированные на этот срез. существующих дел. И это должно быть дополнено более широким углом обзора рыночных злоупотреблений. То есть более широким углом. У нас есть существующие проекты в рамках нашей команды OCTO. Один из них - Metrica — это платформа для измерения данных.

В ближайшие дни и месяцы мы узнаем об этом больше. И еще одно исследование - INFERMAL, которое проводится для оценки предпочтений злоумышленников. Это лишь некоторые из тех работ, которыми мы занимаемся внутри компании. Мы также, как упомянула Летиция, продолжаем искать способы обмена передовым опытом с помощью таких платформ, как эта. Так что мы благодарим вас за приглашение. Будем продолжать в том же духе. Спасибо.

OWEN FLETCHER: Спасибо, Мукеш. Я думаю, что для нас очень полезно получить мнения, исследования и анализ широкого круга заинтересованных сторон по этому вопросу, чтобы GAC мог на основе фактов обсудить возможные дальнейшие шаги, как вы и другие отметили, поскольку поправки к договорам должны стать лишь одним шагом из многих последующих. Итак, мы выделили время для вопросов и ответов, прежде чем перейти к обсуждению GAC. Нико, могу ли я снова обратиться к вам для получения вопросов от членов GAC? Спасибо.

NICOLAS CABALLERO: Спасибо вам большое, Оуэн. Спасибо, Мукеш. И спасибо участникам дискуссии, Редж, Деннису и Джеффу. В данный момент у меня нет никого из участников онлайн или в зале. Так что позвольте мне передать слово Мартине, чтобы она провела нас по обсуждению GAC. Мартина, вам слово.

MARTINA BARBERO: Я заметила поднятую руку.

NICOLAS CABALLERO: Да, это Европейская комиссия. Вам слово, пожалуйста.

GEMMA CAROLILLO: Спасибо, Нико. Я буду краткой. У меня есть вопрос к докладчику, я полагаю, из компании Verisign. Надеюсь, я не... Да, это вы. Вы упомянули, что изучаете возможные направления развития политики. Вы упомянули один пример взаимодействия с сообществом. Я хотела узнать, есть ли у вас уже несколько идей, потому что мы обсуждаем то же самое в GAC. Было бы очень полезно обменяться мнениями. Спасибо.

DENNIS TAN: Спасибо за вопрос, Гемма. Мы изучаем следующий пункт для работы. Не обязательно процесс разработки политики, потому что в начале, несколько месяцев назад, я думаю, мы слышали от

сообщества, что процесс разработки политики очень трудоемкий, громоздкий и требует много ресурсов. Именно поэтому возникла идея о том, чтобы люди могли целенаправленно и узко сфокусировать PDP, что и было сделано. Так что PDP - это один из возможных путей развития. Это то, что мы пытаемся изучить, обсуждая с сообществом ICANN. Мы хотим узнать больше из отчета INFERMAL, который был только что опубликован. Я только бегло ознакомился с ним. Я еще не изучил его, но я верю, что он поможет, станет катализатором для разговоров, которые мы, конечно же, приветствуем.

NICOLAS CABALLERO: Спасибо вам большое за это. У меня на очереди США.

OWEN FLETCHER: Спасибо. Это снова Оуэн Флетчер (Owen Fletcher). Вкратце, я хотел бы отметить, что, насколько я помню, Правление в свое время предлагало созвать заседания по обсуждению возможных вариантов PDP, которые могли бы учитывать более детальные соображения, вытекающие из поправок, и принять по ним последующие меры. Я думаю, нам было бы интересно узнать любую информацию об этом, хотя это, вероятно, не вопрос для всех присутствующих.

NICOLAS CABALLERO: Конечно.

REG LEVY: Это Редж Леви (Reg Levy), я представляю подгруппу по злоупотреблениям DNS Группы заинтересованных сторон регистраторов. Мы с Деннисом, как сопредседатели подгрупп по злоупотреблению DNS Палаты сторон, связанных договорными обязательствами, проводим заседания, которые не обязательно... не обязательно спонсируются Правлением, но мы обращаемся к различным членам сообщества, различным официальным и неофициальным группам внутри сообщества, чтобы выяснить у каждого из них, что они хотят от нас, что они видят, какие тенденции их интересуют и как мы, как договорные стороны, можем принять это и не обязательно превратить это в PDP, но заседания, на которых мы ведем эти разговоры.

Мы уже встречались с ALAC. В ближайшее время мы надеемся встретиться с SSAC, чтобы, опять же, провести индивидуальные беседы, так что у каждой из различных групп в сообществе будет возможность поговорить с нами напрямую.

NICOLAS CABALLERO: Спасибо, США. Спасибо, Редж. Других желающих нет, так что позвольте мне предоставить слово Мартине Барберо (Martina Barbero) из Европейской комиссии, которая расскажет нам о следующих шагах и о том, какие соображения могут возникнуть по поводу Коммюнике. Мартина, вам слово.

MARTINA BARBERO: Большое спасибо, председатель. На самом деле, у нас есть еще две короткие части повестки дня, прежде чем мы вас отпустим и отправимся на обед. Я знаю, что это последняя часть перед обедом, но, пожалуйста, потерпите, потому что это важно. Сначала мы хотели бы предоставить слово для обсуждения того, что мы только что услышали сегодня. Мы подготовили несколько вопросов для обсуждения, чтобы узнать, есть ли у вас какие-либо мнения, которыми вы хотели бы поделиться. В основном мы хотели бы обсудить в рамках GAC, есть ли у вас какая-либо реакция на сегодняшний брифинг о реализации и влиянии поправок к договорам. Я думаю, мы услышали много интересного. Так что, если у вас есть комментарии или замечания, которыми вы хотели бы поделиться, это был бы подходящий момент.

Также мы хотели бы узнать, есть ли еще какие-либо уроки, извлеченные из предыдущего раунда, которые помогли бы нам подготовиться к следующему раунду в отношении борьбы со злоупотреблениями DNS. Думаю, мы услышали немного. Вчера мы кратко говорили о PIC и RVC со сторонами, связанными договорными обязательствами, но есть также, и меня там не было, очень хороший отчет о злоупотреблениях DNS из предыдущего раунда, в котором есть некоторые выводы, которые мы можем взять на вооружение при подготовке к следующему раунду.

И, наконец, поскольку мы услышали очень хорошую презентацию от наших турецких коллег, если есть еще какие-либо передовые практики в области ccTLD, которые можно было бы рассмотреть и которые могли бы стать пищей для размышлений в пространстве

gTLD. Это тоже подходящий момент, чтобы поделиться ими. Так что, прежде чем мы перейдем к рассмотрению коммюнике, Нико, возможно, мы сможем открыть слово по этим вопросам и узнать, есть ли какая-либо реакция со стороны членов GAC. Спасибо.

NICOLAS CABALLERO: Спасибо за это, Мартина. Итак, открываем прения. Мы с радостью примем любые вопросы, комментарии или все, чем вы хотели бы поделиться с нами в данный момент. У меня Индия. Вам слово, пожалуйста.

T. SANTOSH: Спасибо, председатель. Это Сантош для протокола. Во время ICANN80 мы предложили сделать внедрение DNSSEC обязательным, в частности, в таких секторах, как финансы, финансовые услуги, здравоохранение, правительство и телекоммуникации. Это будет соответствовать глобальным мерам безопасности и обеспечит защиту жизненно важной национальной инфраструктуры. Что вы думаете по поводу внедрения DNSSEC? Спасибо.

REG LEVY: Это Редж Леви (Reg Levy) из компании Tucows. DNSSEC - это один из способов защиты доменных имен, а HTTPS, похоже, является принятым в настоящее время протоколом безопасности, который рынок решил, что это то, что ему нужно. Мы предлагаем DNSSEC. Мы с радостью присвоим DNSSEC любому доменному имени,

которое будет у нас куплено. Это не очень популярная опция. Это не та точка зрения безопасности, которой многие наши клиенты, похоже, заинтересованы в использовании преимуществ, как, как я уже сказала, HTTPS. Вы также заметите, что многие браузеры начинают требовать HTTPS, что также способствует развитию этой технологии.

Я не вижу проблемы в том, чтобы просить определенные сектора, поощрять определенные сектора... Извините, мне сказали притормозить. Я не вижу проблемы в том, чтобы попросить определенные отрасли рассмотреть дополнительные пути обеспечения безопасности. Но я обнаружила, что большинство клиентов не заинтересованы в DNSSEC в той степени, в которой, возможно, мы в ICANN хотели бы, чтобы они были заинтересованы.

NICOLAS CABALLERO: Спасибо за это, Редж. У меня на очереди Великобритания.

CHRIS: Да, здравствуйте. Просто представлюсь. Я - Крис. Я впервые в ICANN, но здесь я из Великобритании, в частности, из Рабочей группы по обеспечению общественной безопасности. Я просто хотел бы прокомментировать, основываясь на замечании Индии, что, с точки зрения общей картины, всего несколько дней назад, в прошлую пятницу, под нашим председательством в Совете Безопасности ООН, в этом месяце, мы были председателем заседания по борьбе с вымогательством. И довольно много стран-

членов ООН подписали заявление, в частности, о воздействии на CNI и здравоохранение, в частности, о вымогательстве, но, очевидно, как форма вредоносного ПО, оно очень актуально для этой дискуссии здесь.

Так что, я думаю, в настоящее время растет интерес к этому вопросу со стороны многих членов СБ ООН. Это также распространяется на такие организации, как Инициатива по борьбе с вымогательством, в которой, опять же, Индия принимает активное участие наряду с Великобританией и другими странами в зале. Это не столько вопрос, сколько комментарий к тому, что другие многосторонние организации, в которых участвует ряд членов правительства, продвигают эти вопросы в повестку дня. Тот факт, что он был включен в СБ ООН в это время, очевидно, весьма актуален. Я думаю, будет сделан больший акцент, конечно, через PSWG, на том, что нам, возможно, необходимо рассмотреть риски для конкретных секторов CNI и продвигаться вперед в этом направлении. Спасибо.

NICOLAS CABALLERO: Спасибо вам за это, Великобритания. Следующие США.

OWEN FLETCHER: Спасибо. Это Оуэн Флетчер (Owen Fletcher), США. Я хотел бы коротко ответить и по поводу DNSSEC. Я припоминаю, что на ICANN80 у нас был текст в Коммюнике, который, как я думаю, был составлен после того, как Сантош задал вопрос об этом в то время.

Мы можем просмотреть текст, но я думаю, что просто скажу, что в нашем тексте отмечалась поддержка принятия DNSSEC, что кажется мне хорошей идеей в целом. Но я не уверен в идее призыва сделать его обязательным. Кажется, что нам нужно... прежде чем рассматривать это, нам нужно получить больше информации и быть хорошо осведомленными о последствиях и о том, будет ли это осуществимой идеей.

Я также вспомнил, что SSAC отметил на двустороннем заседании с нами, что они внимательно следят за этой темой, так что они могут быть хорошим источником информации, если мы решим, что хотим получить больше информации. Спасибо.

NICOLAS CABALLERO: Спасибо за это, США. Я не вижу других участников онлайн или в зале. Позвольте мне вернуться к Мартине Барберо (Martina Barbero) из Европейской комиссии, чтобы обсудить дальнейшие шаги и все соображения, связанные с коммюнике, о которых мы должны знать на данный момент. Вам слово.

MARTINA BARBERO: Большое спасибо, Нико. И спасибо всем членам GAC, которые выступили сегодня. Я думаю, Кристофер сделал хорошее напоминание о том, что эта тема занимает важное место в повестке дня, так что мы обязательно примем это во внимание. И это подводит нас к рассмотрению коммюнике. Так что, если можно, перейдите к следующему слайду.

Напомню, что в качестве ведущих по темам мы поместили на слайдах некоторые возможные элементы для размышления, но вклад в это должны внести вы, члены GAC. Как всегда в Коммюнике, у нас есть возможность высказать рекомендации или обсудить важные вопросы. Что касается элементов, которые можно было бы включить в Коммюнике, то после презентации, которую мы провели по реализации поправок к договорам и оценке их эффективности, мы могли бы предложить продолжить работу над этим в качестве GAC. Я думаю, это было бы интересно.

И, конечно, я думаю, мы уже слышали об этом сегодня утром от ALAC, а сегодня, возможно, ожидается дальнейшая работа, будь то в области политики или чего-то еще. Напомню, что, когда был период общественных комментариев по поправкам к договорам, GAC подготовил ответ, в котором указал на некоторые темы, которые могут послужить основой для дальнейшей работы. Они перечислены здесь. Проактивный мониторинг, повышение транспарентности, периодический пересмотр определения злоупотребления DNS, решение проблемы злоупотребления DNS в ICANN и за ее пределами, руководство по ключевым терминам, рассмотрение вопросов обеспечения выполнения договорных обязательств.

Простите, простите, простите. Вы совершенно правы. Я хотела поднять вопрос, чтобы как можно быстрее дать слово для высказываний и комментариев, моя ошибка. Это лишь некоторые из тем, которые были включены в... это темы, которые были включены в ответ на публичные консультации по поправкам к

договорам в то время. А затем в Кигали и также вчера мы немного обсудили соображения по поводу подготовки к следующему раунду TLD, который откроется в ближайшее время.

Так что все эти элементы могут войти в коммюнике. Но смысл следующих восьми минут в том, чтобы понять, есть ли в них те моменты, которые вы считаете важными. Если есть что-то еще, или у вас есть другие соображения, которыми вы хотите поделиться, прежде чем мы перейдем в режим составления коммюнике. Большое спасибо.

NICOLAS CABALLERO: Спасибо за это, Мартина. Так что, можно начинать. Есть комментарии, мысли, вопросы? США, Вам слово.

OWEN FLETCHER: Говорит Оуэн Флетчер (Owen Fletcher), США. Сегодня уже упоминался неофициальный отчет, и кто-то ранее, возможно, это был Джефф, также упомянул домен Metrica, готовящуюся платформу OCTO. Так что, возможно, мы отметим наш интерес к дальнейшим источникам информации и исследованиям, которые могли бы помочь нам определить возможную будущую работу над поправками к злоупотреблениям DNS. Кроме того, я уже упоминал о заседаниях, и Редж отметила, что стороны, связанные договорными обязательствами, также хотят получить информацию об этом. Возможно, GAC может проявить интерес к дальнейшему взаимодействию по этому вопросу. Спасибо.

NICOLAS CABALLERO: Спасибо, США. Следующей у меня Европейская комиссия.

GEMMA CAROLILLO: Спасибо, Нико. Гемма Каролилло (Gemma Carolillo). Я хотела бы поддержать слова Оуэна о том, что мы могли бы поразмышлять над заседаниями, которые состоялись вчера и сегодня. Так что, я думаю, в GAC был большой интерес к отчету SSAC, в том числе о влиянии новых технологий на злоупотребления DNS. Я думаю, что мы должны... Я имею в виду, что было действительно много вопросов и заинтересованности в продвижении этой работы. Кроме того, я думаю, что предложение ALAC о том, чтобы две группы работали бок о бок по теме, представляющей взаимный интерес, приветствовалось, в частности, в связи с темой отчета. Злонамеренно зарегистрированные доменные имена. Но я думаю, что эта тема в целом представляет собой общую обеспокоенность для ALAC и GAC. Спасибо.

NICOLAS CABALLERO: Спасибо, Европейская комиссия. Есть еще комментарии или вопросы? Да, пожалуйста, Вам слово.

SAMANEH TAJALIZADEHKHOOB: Спасибо всем за презентации. Я Самане, директор по исследованиям исследовательской группы SSR в корпорации ICANN. Так как это название всплывало пару раз, мы являемся

руководителями проекта ICANN Domain Metrica, а также группой, финансирующей проект INFERMAL. Я хотел пригласить вас на завтрашнее заседание в 1:15, посвященное обновлению информации о злоупотреблениях DNS, где мы расскажем об обоих проектах, о полученных отзывах и о том, что мы собираемся сделать в качестве следующих шагов. Спасибо.

NICOLAS CABALLERO: Спасибо вам большое за приглашение, Самане. К сожалению, у GAC будет заседание. Мы будем готовить коммюнике завтра в 13:15, но спасибо вам большое за приглашение, хотя это и не мешает никому присутствовать. Конечно. Спасибо вам большое. Следующей у меня Великобритания.

NIGEL HICKSON: Да, спасибо, господин председатель. Очень коротко. Это действительно прекрасный диалог. Я просто хотел спросить, то есть, очевидно, у нас нет времени, чтобы затронуть это сейчас, и это новый вопрос, но на предыдущих заседаниях, когда мы обсуждали RDRS и рассматривали это, мы также отметили диалог, который имел место о создании своего рода мини PDP или микро PDP по конкретным аспектам злоупотребления DNS, таким как фишинг и вредоносное ПО. И это в целом приветствовалось членами GAC. Это не было продолжено. Я знаю, что у людей на повестке дня много других вопросов, и не в последнюю очередь это касается политики GNSO. Но я думаю, что нам нужно вернуться к этому вопросу, потому что, очевидно, есть конкретные проблемы

по некоторым из этих вопросов, по некоторым из этих аспектов злоупотребления DNS. Спасибо.

NICOLAS CABALLERO: Спасибо, Великобритания. Принято к сведению. Есть другие комментарии? Я не вижу других рук в зале или онлайн. Так что позвольте мне предоставить нашим уважаемым участникам дискуссии или Европейской комиссии, правительству США, Редж, кому угодно возможность высказать последние замечания. Слово за вами.

GEMMA CAROLILLO: Хочу поблагодарить всех делегатов GAC, принявших участие в сегодняшней дискуссии. Большое спасибо. Со-ведущие по темам могут предложить некоторые тексты для Коммюнике. Возможно, в разделе «Важные вопросы» речь пойдет о теме, которая остается важной для GAC. Мы подготовим некоторые предложения для вашего рассмотрения.

NICOLAS CABALLERO: Спасибо вам, Европейская комиссия. Любые заключительные замечания от наших уважаемых гостей?

DENNIS TAN: Спасибо, Нико. Я благодарен за приглашение и участие в этом разговоре. Мы считаем его очень важным. Мы с Редж всегда на связи. Любые обсуждения, повторюсь, поправки были первым

шагом. И теперь мы с нетерпением ждем следующих обсуждений. И неважно, будет ли это PDP или что-то другое, мы хотим быть частью этого процесса. Спасибо.

NICOLAS CABALLERO: Спасибо вам большое за это. Джефф, Хаджиме... Вам слово, Джефф.

JEFF BEDSER: Я также хотел бы воспользоваться возможностью и поблагодарить за приглашение, за возможность поговорить на эту тему с этой группой людей. Спасибо.

NICOLAS CABALLERO: Спасибо вам большое, Джефф. Махмут, Хаджиме?

HIJAME ONGA: Большое спасибо за плодотворную дискуссию. Это мой первый раз, но ситуация действительно запоминающаяся. Со следующего заседания я хотел бы сделать все возможное. Спасибо вам большое.

NICOLAS CABALLERO: Спасибо, Хаджиме. Махмут?

MAHMUT ESAT YILDIRIM: Спасибо вам большое за предоставленную возможность поделиться с вами нашим опытом, и мы надеемся увидеть вас здесь снова, чтобы обменяться информацией и поделиться опытом. Спасибо.

NICOLAS CABALLERO: Спасибо, Махмут. Мы надеемся, что скоро вернемся в Стамбул. У меня на очереди Колумбия.

THIAGO DAL-TOE: Спасибо, Нико. Спасибо всем. Хочу напомнить тем, кто присоединился к нам, и не знает, что злоупотребление DNS - это одна из тем нашей стратегической задачи, фактически номер четыре. И я хотел поблагодарить ведущих по темам за организацию этого замечательного заседания и надеюсь, что мы сможем продолжить работу над этим вопросом. Спасибо.

NICOLAS CABALLERO: Спасибо вам большое. Заседание закрыто. Пожалуйста, вернитесь ровно в 1:15 для встречи с Правлением. Спасибо вам большое. Приятного обеда.

[КОНЕЦ СТЕНОГРАММЫ]