ICANN69 | Виртуальное ежегодное общее собрание – Борьба со злоупотреблениями DNS
20 октября 2020 года, 10:30 — 12:00 по CEST

ВЫСТУПАЮЩИЙ: Тест для сотрудников нашего отдела лингвистического обеспечения.

Устный перевод этой сессии будет осуществляться в Zoom и на удаленной платформе синхронного перевода под управлением Congress Rental Network. Рекомендуем загрузить приложение Congress Rental Network в соответствии с инструкциями в чате Zoom или из документа со сведениями о конференции на странице веб-сайта конференции. Если вы хотите говорить, поднимите руку в комнате Zoom, и после того как координаторы конференции назовут ваше имя, наша команда технической поддержки даст вам возможность включить микрофон. Назовите для протокола свое имя. Если вы говорите на языке, отличном от английского, назовите свой язык. Когда будете говорить, отключите звук на всех прочих устройствах и в приложениях, включая приложение Congress Rental Network. Пожалуйста, говорите разборчиво и с нормальной скоростью, чтобы обеспечить точный перевод. Конец теста аудио.

Сообщите, если это сообщение нужно прочесть еще раз. Спасибо.

ВЫСТУПАЮЩИЙ: Здравствуйте и добро пожаловать! Мы начнем всего через минуту. Спасибо.

ВЫСТУПАЮЩИЙ: Сессия начинается, включите запись.

ОЗАН САХИН (OZAN SAHIN): Приветствую всех и добро пожаловать на пленарное заседание по предотвращению злоупотреблений DNS. Меня зовут Озан Сахин, я являюсь менеджером удаленного участия на этой сессии. Обратите внимание, что выступления записываются, и мы придерживаемся стандартов ожидаемого поведения ICANN.

Во время заседания будут зачитываться только вопросы и комментарии на английском языке, присланные с использованием панели вопросов и ответов. Эта функция доступна в панели инструментов Zoom. Я зачитаю вопросы и комментарии вслух во время, отведенное председателем или модератором этого заседания.

В ходе этой сессии также ведется стенограмма, и устный перевод в реальном времени. Чтобы смотреть стенограмму в реальном времени, нажмите кнопку субтитров на панели инструментов Zoom. Устный перевод сессии на арабский, китайский, английский, французский, русский и испанский языки ведется в Zoom и на удаленной платформе синхронного перевода под управлением Congress Rental Network. Участникам рекомендуем

загрузить приложение Congress Rental Network в соответствии с инструкциями в чате Zoom или из документа со сведениями о конференции на странице веб-сайта конференции.

Если вы хотите говорить, поднимите руку в комнате Zoom, и после того как координаторы конференции назовут ваше имя, наша команда технической поддержки даст вам возможность включить микрофон. Назовите для протокола свое имя и язык выступления, если это не английский. Когда будете говорить, отключите звук на всех прочих устройствах, включая приложение Congress Rental Network. Говорите разборчиво и в нормальном темпе, чтобы обеспечить точный перевод.

Хочу отметить, что удаленные участники не могут нажимать на кнопку микрофона и включать собственный звук во время собрания без соответствующего разрешения команды технической поддержки. Все участники собрания могут оставлять комментарии в чате. Для этого воспользуйтесь раскрывающимся меню в панели чата и выберите «Ответить всем участникам группы и присутствующим», чтобы ваш комментарий был виден всем. Обратите также внимание, что закрытые чаты возможны только для участников публичной дискуссии в формате вебинара Zoom. Сообщения, отправленные обычными присутствующими, будут видны организаторам, -соорганизаторам и другим участникам публичной дискуссии. Теперь я передаю слово Томасу Рикерту. Томас?

ТОМАС РИКЕРТ (THOMAS RICKERT): Большое спасибо, ОЗАН. И доброе утро, добрый день, добрый вечер всем, меня зовут Томас Рикерт. Я являюсь директором по именам и номерам в германской ассоциации интернет-отрасли, которая является одним из со-организаторов ICANN69, и хотел бы виртуально пригласить вас в мою родную Германию. Я нахожусь в БОННЕ. Мне очень хотелось бы приехать в Гамбург, чтобы увидеть вас лично, но, к сожалению, это невозможно в текущей ситуации. Надеюсь, что у нас будет возможность пообщаться в ближайшем будущем и что все здоровы. Давайте перейдем к следующему слайду.

Как уже сказал ОЗАН, темой этой сессии является борьба со злоупотреблениями DNS. В истории ICANN в Бонне уже было проведено много сессий по злоупотреблению DNS, и эта тема остается актуальной, и мы занимаемся ей, потому что в интернете происходит очень много всего плохого. Очень много злоумышленников пользуются недостатком знаний пользователей и заманивают пользователей на сайты с недобросовестными предложениями, которые пользователям видеть не стоит, и причиняют этим финансовые и другие убытки. Для ICANN эта тема имеет особое положение в виду очень ограниченного мандата ICANN согласно Уставу. По этой причине важно продолжать диалог по борьбе со злоупотреблением DNS, чтобы понять, в чем заключается сама проблема, понять, какие роли и ответственность несут различные игроки в экосистеме

интернета, а также какие решения могут быть потенциальные и имеющиеся решения.

Я надеюсь, что в течение этой сессии нам удастся решить ряд вышеупомянутых вопросов, и попробуем сосредоточиться на решениях и возможных дальнейших путях. Продолжительность сегодняшней сессии 90 минут. На ней выступят с презентациями несколько человек, которых я представлю вам уже очень скоро. Затем после каждой презентации мы сделаем паузу, чтобы ответить на вопросы в панели вопросов и ответов. Мы постараемся ответить на ваши вопросы. Постарайтесь задавать вопросы по теме прослушанной презентации, и, если что-то останется неясным, то выступающий сможет ответить вам. В конце этой 90-минутной сессии после докладов мы проведем сеанс вопросов и ответов, где у вас будет возможность задать более общие вопросы. Сделать это вы сможете как в панели комментариев, так и просто подняв руку в комнате и включив свой микрофон по разрешению команды технической поддержки, чтобы вы могли комментировать -- вслух. Я заканчиваю вступительные заметки, и мы сможем поговорить на тему сессии -- уже через несколько секунд. Чтобы вы знали, кто сегодня будет делать доклады на тему борьбы со злоупотреблениями DNS, мы сначала заслушаем Давида Конрада (David Conrad) и затем Джеффа Бедсера (Jeff Bedser). Также доклады сегодня сделают Мейсон Коул (Mason Cole), Крис Льюис-Эванс (Chris Lewis-Evans), Джеймс Блейдел (James Bladel).

После этого мы проведем обсуждение, на котором, я надеюсь, вы зададите вопросы, затем за несколько минут до конца я постараюсь подвести итог всего того, что мы услышим. Давайте перейдем к следующему слайду, на котором представлен обзор -- вот, это уже первый слайд Давида. Итак, из этого слайда вы уже можете получить представление о том, что мы будем сегодня обсуждать, и сейчас я хотел бы передать слово Давиду Конраду для доклада о новинках ICANN в отношении борьбы со злоупотреблениями DNS. Давид, вам слово.

ДАВИД КОНРАД (DAVID CONRAD): Спасибо, Томас. Следующий слайд, пожалуйста. При подготовке к этому пленарному заседанию я по отдельной просьбе подготовил слайды, на которых попытался показать угрозу безопасности доменов в период с сентября 2019 года до сентября 2020. Если вы заглянете в отчеты DARR, т.е. в отчеты по активности DNS, доступные на веб-сайте ICANN, то в данных этих отчетов представлена информация за последние 9 месяцев, прошу прощения за опечатку. Однако меня попросили представить данные за один год. Поэтому моя команда составила общую статистику. За этот год мы наблюдали понижение активности фишингового вредоносного ПО и сетей зараженных машин (ботнетов) и повышение СПАМ-активности. Преобладание СПАМА при рассмотрении статистики злоупотребления DNS все несколько искажает.

В целом за 2019-2020 гг. показатель неправомерного использования доменов повысился на 13%, однако, общий показатель остался приблизительно на одном уровне в результате спада всех других составляющих показателей. Следующий слайд, пожалуйста. Однако данные, которыми располагает DARR, датируются даже октябрем 2017 года, и если заглянуть еще дальше, то можно увидеть некоторые совершенно очевидные тенденции. Графики трендов показывают, что количество gTLD повышается, и со временем можно увидеть как спады, так и подъемы, однако вырисовывается достаточно четкая тенденция. На графике №2 показано общее количество угроз безопасности, все показатели, которые мы рассматриваем в проекте DARR, т.е. контроль сообщества над ботнет. Распределение фишингового вредоносного ПО и СПАМа. Здесь видно, что тенденция явно идет на спад. На графике 3 видно, и в целом нормализация выполняется по количеству доменов в определенной зоне, в общем, на графике виден спад по времени и небольшой рост в конце графика. Далее на графике 4, где красным обозначен СПАМ, показано, что СПАМ доминирует по всем показателям. Еще один момент на графике 4 заключается в том, что определенном месте на синем и красном графиках можно увидеть момент вступления в силу регламента GDPR. Также на этих графиках не видно никакого существенного изменения числа случаев неправомерного использования доменов, по

крайней мере, в контексте DARR. Следующий слайд, пожалуйста. Если посмотреть на отдельные угрозы за тот же период, начиная с октября 2017 года по октябрь 2020 года, то, опять же, видно, что на графиках трендов имеются любопытные моменты. Это в сравнении со статистикой, предоставленная мной на первом слайде, на котором видно, что число случаев использования фишингового ПО и ботнетов шли на спад. Если мы вернемся к -- 20 октября 2017 года, то мы увидим противоположную картину: использование фишингового ПО и ботнетов растет, но медленно. А СПАМ за тот же период времени - претерпевает существенный спад. Одна вещь, на которую стоит обратить внимание на этих графиках, – это правильное сопоставление осей Y. Все эти графики СПАМа имеют иной порядок величины, который выше чем все другие. Поэтому на этом нужно заострить внимание. Следующий слайд. Еще один набор данных, который мы собираем в офисе технического директора, – это индикаторы работоспособности технологий идентификаторов. Сбор этих данных мы начали в январе 2018 года. Мы наблюдаем за большим количеством показателей, имеющих отношение к надлежащей работоспособности экосистемы идентификаторов. В этом наборе метрик имеется один специфический поднабор, метрика M2, касающийся неправомерного использования доменных имен. В нем отображены тенденции, начиная с января 2018 года со

случаями неправомерного использования на 10 000 доменов в gTLD и регистраторах, на которые в целом приходится 50-90% угроз безопасности. Если посмотреть на эти таблицы -- на сайте ITHI, интерфейс которого может напомнить вам дизайн начала 90-х годов, то уровень злоупотреблений на этом сайте составляет, например, для фишинга 10% -- 10 регистратур приходится на 90% фишинговых угроз безопасности, которые удалось выявить. Эти показатели составляют 0,3% на регистратуру и 0,1% этих данных регистраторов могут быть неправдивыми или некорректными. Информация о регистраторах в нашем распоряжении предоставлена нашим поставщиком, iThreat. Она накапливается в базе за определенный период времени, поэтому у нас нет доступа из системы DARR к информации регистратора, связанной с отдельными доменами. Эта информация может быть устаревшей, поэтому ее следует использовать как некий индекс, а не рассматривать, как точные значения. Также должен подчеркнуть, что -- метрики ITHI выводятся из тех же необработанных данных, которые используются и в DARR, плюс некоторая информация о регистраторах. Следующий слайд, пожалуйста. Еще один проект, который мы ведем в офисе технического директора, и который имеет отношение к борьбе со злоупотреблением DNS – это проект под названием «сбор идентификаторов угроз безопасности доменных имен», сокращенно DNSTICR. Этот проект был запущен в январе

2020 года. Его целью являлся сбор информации, касающейся доменов, -- которые были зарегистрированы с целями, имеющими отношение к пандемии. В самом начале пандемии имелось было определенное количество отчетов -- о потоке регистраций, связанных с пандемией, с определенным пониманием, что эти регистрации используются в неправомерных целях. В DNSTICR мы наблюдали только за распространением фишингового и вредоносного ПО, как за угрозой безопасности. В период с мая 2020 -- года по сентябрь 2020 года мы целенаправленно собирали данные и анализировали их. С помощью нашей системы мы определили, что из 134 000 выявленных регистраций 1,7% -- обладали всеми признаками, по которым мы могли отнести их к категории неправомерного поведения. И в июне мы уже фактически начали сообщать о таких доменах регистраторам. Следующий слайд, пожалуйста. Если рассмотреть все, что мы нашли в течение отчетного периода с июня 2020 года по сентябрь 2020 года, то было зарегистрировано 80 000 доменов, имеющих отношение к пандемии. Из них 170 регистраций привели к отправке регистраторам отчетов -- с указанием, что с нашей точки зрения имеются признаки поведения, представляющего угрозу безопасности, и небольшое пояснение -- это означало, что доменное имя было зарегистрировано в системе доменных имен. Также имелся минимум один определенный отчет в одном из списков поставщиков. И когда мы посмотрели на

фактические регистрационные данные, то домен, -- прошу прощения, сайт, привязанный к домену, содержал материалы, указывавшие -- на определенного рода угрозу безопасности. Также мы хотели снизить количество ложных отчетов, поэтому по состоянию на 6 октября, из этих 170 выявленных регистраций в системе доменных имен 87 уже не существуют. Они были удалены. 56 из них более не соответствуют критериям отчетов. Либо домен не распознается, либо на соответствующих сайтах более не обнаруживаются признаки угрозы безопасности. Для 20 из них больше не распознается имя, а запись NS для DNS-серверов больше не отвечает на запросы DNS. 7 доменов из 170 все еще являются угрозой. Теперь буду рад ответить на любые вопросы и передаю слово Томасу. Если нет, то представляем следующего докладчика.

ТОМАС РИКЕРТ: Большое спасибо, Давид. Мы -- [неразборчиво] У нас есть пара вопросов. Не уверен, сможем ли мы ответить на все вопросы сейчас, но давайте попробуем. Элизабет Шуди (Elizabeth SZUDI) задает вопрос по поводу СПАМА. Представляет ли это незапрошенные э-лектронные письма или СПАМ - также содержит другие формы технологических [неразборчиво] или фишинга, содержат ли и доставляют ли СПАМ-письма другие формы злонамеренного контента?

ДАВИД КОНРАД: Информация в нашем распоряжении получена от поставщиков с хорошей репутацией. Они не делают различий между механизмами, используемыми в СПАМе для доставки угроз безопасности. Здесь представлена информация, касающаяся СПАМа, о которой сообщают различным поставщикам, пользующимся доверием. В наших отчетах DARR и в документах по методологии мы приводим список проверенных поставщиков, с которыми мы работаем, и конкретные данные этих проверенных поставщиков, чтобы дать вам понимание, какую интерпретацию мы собираем.

ТОМАС РИКЕРТ: Спасибо, еще два вопроса. Члены моей группы говорят о повышении числа случаев неправомерного использования доменов в результате неправомерного использования названий брендов. Мне кажется, что рост числа неправомерных действий должен также отразиться и на показателях фишинга. Немалая часть фишинга также распространяется через Snapchat. Каким образом эти показатели это отражают? Должны ли они идти параллельно, и вопрос в до-гонку касательно 10 регистратур с самыми плохими показателями, какие меры будут предприняты касательно их? Их статус на сегодня, спасибо.

ДАВИД КОНРАД: Что касается корреляции между фишингом и СПАМом, то собираемая нами информация основывается на данных, предоставляемых соответствующими поставщиками. Если в каких-либо данных что-то указывается в категории СПАМ, и это фишинг, и он распространялся через фишинг, то, возможно, эти данные появятся в двух различных категориях, потому что они отражены в нескольких местах. Мы стараемся удалять дубликаты, имеющие такую природу, но могут встречаться случаи, когда дубликаты таких данных все же остаются. Насколько мне известно, это маловероятно. Никакую собираемую нами информацию мы не изменяем. Эту информацию мы получаем от целого ряда различных поставщиков, и если мы видим статистику касательно злоупотребления DNS и угроз безопасности, то мы выясняем источники данных, использованные для получения этой информации. Мы также можем воспользоваться системой DARR и выяснить, можем ли мы загрузить эти данные в систему DARR и другие системы, которыми мы пользуемся. Что касается второго вопроса, то давайте посмотрим -- абсолютное количество регистратур или регистраторов, несущих ответственность за 90% всех злоупотреблений, -необходимо понимать в контексте ненормализованных данных. Возможно, это не новость, что имеется очень сильная связь между общим количеством регистраций и количеством злоупотреблений в числе этих регистрации. При взгляде на ненормализованные

данные видно, -что регистратуры и регистраторы с самым большим количеством регистраций, бесспорно, будут содержать самое большое количество доменов, используемых злоумышленниками. Эти данные лучше рассматривать в контексте нормализованных данных, соотносящихся с количеством регистраций. Если смотреть на эти числа, то -- -- ответ на вопрос, кто на самом деле имеет наихудшие показатели, становится менее очевидным.

ТОМАС РИКЕРТ: Большое спасибо. Боюсь, нам нужно переходить к следующему докладу. Давид, я предлагаю, пока мы будем слушать доклад Джеффа, может быть, вы перейдете на панель «вопрос-ответ» и попробуйте ответить на вопросы письменно? То же касается и последующих докладчиков. Когда у нас появятся вопросы, мы попытаемся на них ответить в конце сессии. Общий сеанс вопросов и ответов. Думаю, можно. Джеф Бедзер. И работа с iThreat. Джефф, вам слово. 10 минут.

ДЖЕФФ БЕДЗЕР (JEFF BEDSER): Доброе утро, добрый вечер, добрый день. Это группа, которую учредили в SSAC около года назад. У них был основательный устав. Они включили в него множество разных вопросов по злоупотреблениям DNS, которых мы еще не касались. Это первый рабочий продукт, которые мы

опубликуем, и который покрывает проблемы борьбы со злоупотреблениями DNS. До настоящего момента это работа еще не была опубликована, однако, надеюсь, что этот документ SSAC будет опубликован в течение следующих нескольких недель. Мы надеялись, что опубликуем его до ICANN69, но внутренние процессы не завершены, и мы надеемся, что скоро их закончим. Следующий слайд, пожалуйста. Прежде всего, я хотел бы убедиться, что всем ясно, в этом рабочем продукте мы пригласили гостей из группы аудита SSAC принять участие в рабочем в процессе. Это были гости из PSWG, из группы заинтересованных сторон-регистратур. Некоторые из них поделились навыками и знаниями, которые помогли нам понять лучше некоторые проблемы политики и некоторые проблемы обращения со злонамеренными действиями. Прошу прощения, приложение для перевода только-только запустилось. Итак, группа состоит из людей, которые не входят в SSAC, а также собственно из членов SSAC. Таким образом, мы собрали команду людей, имеющих достаточный опыт в формировании политики. Также у нас работали люди с опытом решения проблем злоупотребления DNS, люди из регистратур, регистраторов и сетей передачи данных, благодаря чему мы достигли очень хороших результатов. Один из моментов, о которых говорил Давид Конрад, – это измерение данных о злоупотреблениях DNS. Одной из проблем этого измерения является не только

сам факт существования злоупотребления в определенный момент, но проблема со злоупотреблением заключается еще и в продолжительности самого злоупотребления. Каждый час или день существования злонамеренного домена увеличивает вероятность появления большего количества жертв. Больше пострадавших приводит к большим убыткам и пр. Далее в презентации мы рассмотрим данные от Криса Льюиса-Эванса по убыткам в результате злоупотребления DNS. Однако сам интернет используется для злоупотребления в масштабах, вызывающих беспокойство. Существует множество отчетов в Правлении, которые можно найти в средствах массовой информации, во внутренних источниках либо в правоохранительных органах, и это говорит о том, что, бесспорно, проблема злоупотребления DNS имеет место. Не стоит ожидать, что злоупотребление DNS прекратится, потому что киберпреступления будут продолжаться. Преступность будет существовать до тех пор, пока существуют потенциальные жертвы. Проблема, которую мы решаем, заключается в том, что разрушается доверие там, где пользователи интернета, будь то коммерческие или частные пользователи или любые другие некоммерческие стороны, какова бы ни была их деятельность, должны доверять системе и поставщикам услуг для обеспечения инфраструктуры. Отчет, который скоро должен быть опубликован, очерчивает стратегию снижения количества злоупотреблений DNS. Целью

является определение оптимальных методов. Этого можно достичь только при сотрудничестве и -взаимопонимании большинства организаций. В DMOOEP считают, что он организации, связанные договорными обязательствами, и ICANN представляют лишь малую часть общего количества систем DNS, с помощью которых осуществляются правонарушения. Это поставщики услуг хостинга. Это поставщики услуг -электронной почты. Это системы передачи данных. Существует огромное количество мест, в которых они используются в структуре, и стороны, связанные договорными обязательствами, представляют лишь малую часть всей экосистемы. Следующий слайд, пожалуйста. Ключевой идеей отчета является следующее. Создание стандартных определений злоупотребления. В документе не предпринимается попытка -переопределения или применения новых определений, но делается шаг от существующих определений, имеющих очень хорошую формулировку в непрофессиональной среде. Они описывают проблему. При попытке решения проблемы наличие набора стандартных определений, конечно, является наилучшим путем продвижения вперед. Следующим вопросом в документе является определение -- первоначальной точки ответственности за устранение злоупотребления. В этом понимании каждый вид злоупотребления имеет свои особенности. Здесь решается вопрос, на каком уровне

инфраструктуры это злоупотребление можно устранить. Возможно, на уровне регистратуры. А может быть на уровне хостинга. Это может быть любой уровень экосистемы, однако, определенные виды злоупотреблений всегда будут происходить, но у каждого злоупотребления есть определенное место, в котором его наиболее «удобно» устранить. Но определение оптимальных методов и разворачивание доказательных стандартов может иметь определенные проблемы. Распространение этих юридических стандартов по юрисдикциям предъявляет различные совершенно очевидные требования для доказательства проблематичности. Например, мошенничество и преступление. Однако при наличии общепринятого стандарта, указывающего, что конкретный инцидент представляет собой случай управления и командования через сеть зараженных машин, то такой стандарт и нужен для доказательства, что это ботнет, любой организации, -- предъявляющей требование действовать в отношении этого конкретного домена ботнета. Установка стандартизированных каналов передачи разрешения проблем на более высокий уровень для устранения злоупотребления, – это как раз тот случай, когда мы все понимаем, что у домена имеется жизненный цикл, т.е. различные действующие лица на пути решения проблемы. Но реальность такова, что в некоторых случаях вы можете встретиться с нереагирующей организацией, являющейся

первичной инстанцией решения проблемы домена. Поэтому установление каналов передачи разрешения проблем на более высокий уровень позволяет различным организациям попасть в экосистему и дать добро поставщику услуг хостинга, -- с которым они в ином случае не могут связаться. У них нет доступа к контактной информации или по имеющимся контактам организация не отвечает. Именно в этом случае каналы передачи разрешения проблем на более высокий уровень очень кстати для следующей стороны, ответственной за разрешение проблемного домена. Опять же, чем продолжительней время работы проблемного домена, тем больше потерпевших. Необходимо определить правильное время для действий и сообщения о злоупотреблениях. На сегодня большая часть ответственных организаций предоставляет сторонам, которым они сообщили о злоупотреблении по каналам передачи разрешения проблем на более высокий уровень, 24 часа на ответ. Итак, если какая-либо организация подает отчет о злоупотреблении определенного домена в неправильной части экосистемы, и потом этот отчет перенаправляется три раза, то в сумме на разрешение проблемного домена требуется 72 часа или больше. Поэтому определение правильного времени для -действия также снижает продолжительность «жизни» проблемного домена. Мы также следим за новостями в сфере программ уведомления, которые будут способствовать и

повышать эффективность определенных частей системы борьбы со злоупотреблениями. Имеется множество коммерческих и --некоммерческих организаций, выявляющих злоупотребления и сообщающих об этом. Есть еще одна интересная тенденция, которую мы заметили в рабочей группе. Она заключается в том, что количество компаний, подающих отчеты о злоупотреблениях, растет так же, как и количество потребителей и брендов, выявляющих злоупотребления и нанимающих другие компании для выявления злоупотреблений. Также имеется большое количество новых игроков, сообщающих о злоупотреблениях для улучшения понимания условий обслуживания и понимания принципа работы DNS-системы. В этом случае очень поможет программа уведомления. …как в рамках GDPR, так и вне. Это касается организаций, фактически располагающихся на различных уровнях управления доменом. Иногда контактную информацию для подачи отчета о злоупотреблении найти просто, а иногда и не очень. Механизм, обеспечивающий программам уведомления простоту поиска контактной информации для подачи отчета о проблемном домене, был бы очень кстати для экосистемы и, в конце концов, обеспечил бы достоверность контактной информации. Поддерживал бы эту информацию актуальной и обновленной. Поддерживал бы ее доступность. Ну и опять же, надеюсь, что этот отчет будет опубликован рабочей группой

для всего сообщества в течение следующих нескольких недель, и надеюсь получить от сообщества обратную связь. Томас, передаю слово снова вам.

ТОМАС РИКЕРТ: Спасибо большое, Джефф. Не смотря на насыщенность твоего доклада, ты отлично уложился в отведенные тебе 10 минут. Прекрасно. Я вижу, что в панели «вопрос-ответ» в основном вопросы, -адресованные Давиду, поэтому, если у вас есть вопросы для Джеффа, оставляйте их там же, и я предлагаю, Джефф, по примеру Давида, попробуй ответить на эти вопросы письменно. Это позволит нам перейти к следующему докладу. Следующий докладчик Мейсон Коул. Мэйсон представляет группу коммерческих заинтересованных сторон и будет говорить от ее имени и с Perkins coin. Он сделает доклад о борьбе со злоупотреблениями DNS с точки зрения CSG. Вам слово, Мэйсон.

МЭЙСОН КОУЛ (MASON COLE): Спасибо, Томас. Вы меня хорошо слышите? Спасибо. Доброе утро, добрый день и добрый вечер всем. Я начинаю. Думаю, все 10 минут мне не понадобятся, но давайте посмотрим. Следующий слайд, пожалуйста. Итак, мы сегодня говорим о борьбе со злоупотреблениями DNS. Это такая проблема, как уже сказал Джефф и другие, которая будет

существовать всегда. Мы видим, что эта проблема повторяется каждый год. Ее масштаб увеличивается внешними событиями, например, вспышка COVID, как мы видели в апреле и марте этой весной. Иногда такое можно наблюдать во время национальных бедствий. Гражданских волнений. Других -всемирных проблем. Но общая тема состоит в том, что DNS используется в незаконных целях. Это уже 4-е заседание ICANN -- четвертое заседание подряд по борьбе со злоупотреблениями DNS. Думаю, всем нам хотелось бы продолжить продуктивное обсуждение, но также нам нужны продуктивные решения, которые мы можем вынести вперед для решения проблемы злоупотреблений DNS и снижение количества таких проблем. Следующий слайд, пожалуйста. Хорошо. Создается впечатление, что все, что нужно сделать для получения статистики, – это просто рассмотреть злоупотребления DNS, структурировать их, и мы увидим всю картину. Последним был опубликован набор данных SSAC Группой по консультациям по промежуточному отчету несколько дней назад. За время этого исследования, продолжавшегося с 1 мая по 31 июля текущего года, акцент был сделан на фишинге, однако, отчеты касались более чем 99 000 уникальных доменных имен, 439 TLD и 414 регистраторов. Из этого числа было выявлено 60 000 доменов, зарегистрированных со злонамеренными целями, поэтому мы знаем, что проблема фишинга имеет место, и она масштабней,

чем об этом сообщается, однако, точный масштаб неизвестен, а сокрытие данных WHOIS создает дополнительные проблемы для обнаружения проблемы. Следующий слайд. Поэтому согласно данным SSAC нам известно, что злоупотребления DNS и киберпреступления продолжаются, нанося вред миллионам пользователей ежегодно, и подрывают доверие пользователей к интернету. Мне хотелось бы подчеркнуть, что Джефф сказал ранее. Это касается доверия к самому фундаменту интернета, можно ли DNS рассматривать, как систему, достойную доверия, из которой можно получать информацию, заниматься бизнесом и выполнять нашу работу. Поэтому для предоставления данных отдельным пользователям, некоммерческим и коммерческим организациям нам необходимо иметь доверие. Следующий слайд, пожалуйста. Спасибо. Это статистика и здесь нам следует прийти к согласию. Думаю, каждый из нас может посмотреть на вопрос со своей точки зрения, так как мы уже провели 4 подобных сессии. Злоупотребление DNS может, как учащаться в зависимости от вашего источника данных, так и понижаться в зависимости от вашего источника данных. Нам нужно прийти к общему знаменателю в том плане, что злоупотребления влияют на доверие к интернету, и нам необходимы профилактические мероприятия по устранению недостатков, основанные на достоверных данных. Ударение здесь на «профилактические». Наши нашей возможности

решать проблемы злоупотребления DNS позволяют нам действовать с большим упреждением и более решительно. И я не хотел бы создать конфликт в ICANN в отношении того -- стоит ли нам агрессивно решать проблемы злоупотреблений DNS, но нам стоит обратить внимание на то, как мы обсуждаем злоупотребления DNS. Не стоит из-за этого начинать перепалку. Нам всем стоит рассмотреть, что мы можем сделать в отношении ненадежных проблемных организаций. Следующий слайд, пожалуйста. Прогресса мы добились, как уже было сказано, и я хотел бы в частности еще раз отметить волонтерскую концепцию, которую регистратуры и регистраторы создали в начале этого года или в прошлом году. Она возымела ощутимое влияние на борьбу со злоупотреблениями DNS и такие действия необходимо поощрять. И я хотел бы воспользоваться случаем и поблагодарить отдел работы со сторонами, связанными договорными обязательствами, за хорошую работу, проделанную ими в этом сценарии. Следующий слайд. Также имеются области, в которых прогресс достигнут не был, и в которых есть над чем поработать. Волонтерские концепции – это хорошо. Однако они не являются инклюзивными в полной мере. И мы знаем, что всегда существуют эти упоминаемые от 8 до 10 организаций, о которых, как говорят в ICANN, они знают, и знают, где они обычно скрываются. Было бы очень полезно решить сначала проблемы, не -требующие множество

ресурсов, а известным проблемным организациям сделать что-то со злоупотреблениями вне этой концепции, созданной сторонами, связанными договорными обязательствами. Следующий слайд, пожалуйста. Давайте вернемся к заседанию в Монреале. То же время в прошлом году, когда мы провели нашу первую пленарную сессию по борьбе со злоупотреблениями DNS. Мне хотелось бы вспомнить доклад представителей Tucows, что мне кажется полезным. Нам необходимо решать проблемы, имеющиеся на расстоянии вытянутой руки, и выполнение -- оно касается соблюдения обязательств ICANN. Если соблюдение требований в состоянии эффективно выявить определенные элементы контракта, которые помогут им осуществлять совершенно очевидные злонамеренные действия, которые, как мы все знаем, имеют место, тогда давайте поговорим о них. Соблюдение обязательств касается известных злонамеренных действий, которые, должны быть устранены. Все с этим согласны. Мне хотелось об этом упомянуть, потому что, опять же, это является упреждающим решением, которое мы можем положить на стол здесь и сейчас, и в котором мы можем использовать некоторые имеющиеся в наличии средства для идентификации злоумышленников и их преследования. Следующий слайд, пожалуйста. Это мой последний слайд. Конечно, нельзя подняться на Эверест одним прыжком. Это делается шаг за шагом поэтапно. Подобным образом мы можем решать

проблему злоупотребления DNS поэтапно. В дополнение к будущим рекомендациям SSAC вот несколько идей, что мы можем сделать с этим -- со злоупотреблениями. Решить проблемы, -которые можно решить быстро, опять же, это 8 из 10 ненадежных организаций, которые создают наибольшие проблемы в этой среде, и решить эти проблемы мы можем сейчас с помощью средств в нашем распоряжении. Мы можем спорить сейчас или позже касательно определения злоупотреблений и нужны ли нам какие-либо средства. Мы можем рассмотреть инициативы для надежных чистых регистратур и регистраторов, возможно, финансовые инициативы, доступные для корпорации ICANN… соблюдение обязательств. Хотелось бы, чтобы стороны, связанные договорными обязательствами, действовали с упреждением. …это не только устранение по факту злоупотребления, но также профилактика возможных случаев. И лично я хотел бы видеть это на том основании, которое мы заложили на данный момент, один раз на пленарное обсуждение мы можем включить это в повестку и рассказать, что мы сделали в отношении злоупотреблений DNS. Это несколько идей, как мы можем продвинуться вперед в течение следующего года и усилить борьбу со злоупотреблениями DNS. Томас, вам слово.

ТОМАС РИКЕРТ: Большое спасибо, Мэйсон. Большое спасибо. У нас два вопроса, адресованные вам. Предлагаю ответить на них перед следующим докладом, и было бы здорово, если бы вы ответили кратко. … кто финансировал…

ДЖЕФФ БЕДЗЕР: Не знаю, извините.

ТОМАС РИКЕРТ: Люк спрашивает, Мэйсон, как вы можете объяснить реакцию WHOIS в выявлении фишинга? Мне кажется, что отследить заинтересованное лицо, стоящее за фишингом, может быть сложно, однако количество злонамеренных доменных имен остается тем же. Спасибо.

ДЖЕФФ БЕДЗЕР: Благодарю за вопрос. Люк, позвольте мне ответить вам письменно. Это -- здесь много всего нужно пояснить и я хотел бы дать более подробный ответ. Томас, вы не против, если я так поступлю?

ТОМАС РИКЕРТ: Разумеется. И еще пара вопросов. Мы можем на них ответить, если вы не против, в панели «вопрос-ответ». Я знаю, что вопрос увидели все. Поэтому, если вы хотите задать вопрос, пробегитесь глазами по вопросам и уточните, не задавал ли

кто-то подобный вопрос до вас, чтобы нам не повторяться с ответами. Следующий доклад делает Кристофер Льюис-Эванс на тему злоупотреблений с точки зрения рабочей группы по общественной безопасности. Крис работает в национальном агентстве по борьбе с преступностью Великобритании. Вам слово.

КРИС ЛЬЮИС-ЭВАНС: Спасибо, Томас, и приветствую всех. Благодарю всех, что присоединились к этому пленарному заседанию по борьбе со злоупотреблениями DNS. Давайте перейдем к следующему слайду.

Зачем мы обсуждаем злоупотребления DNS? Мєйсон и Джефф говорили о различных сессиях и их количестве, и я думаю, что причина проведения этих сессий – это влияние, которое оказывает злоупотребление на пользователей интернета. Поэтому я здесь привожу 5 видов статистики, поясняющие различные типы такого влияния. Различный масштаб злоупотреблений. Хорошую статистику предоставляет центр жалоб по интернету в ФБР. В их статистике приводится количество поступивших жалоб за последний год. Средний показатель составляет 1300 заявлений в день. Также приводятся немалые цифры убытков. Это по всем пользователям интернета. Коммерческие пользователи. Индивидуальные пользователи. Это касается всех. Что касается

национальной статистики, то по нашим записям 85% всех сообщений о мошенничестве говорят о кибермошенниках. Вы видите, какое влияние оказывает злоупотребление DNS, и какой вред это причиняет индивидуальным пользователям интернета. В отношении масштаба причиненного ущерба, то программы-вымогатели, возможно, являются наиболее распространенной формой вредоносного ПО на сегодняшний день. Они оказывают самое большое влияние с приростом в 715% за последний год. Это очень-очень большой прирост причиненного ущерба. Это не только финансовые убытки для индивидуальных и коммерческих пользователей. Злоумышленники также завладевают данными пользователей. В Объединенном королевстве более 60% всех случаев киберпреступлений, имеющих отношение к утечке данных, были совершены с помощью фишингового или вредоносного ПО, что, собственно, и поясняет злоупотребление DNS в данном случае. И это отдельно признается в концепции злоупотребления DNS, о которой упоминал Мэйсон. Что касается -- следующий слайд, пожалуйста. Мне кажется, я видел, как в чате, кто-то по имени Максим, упоминали, что мы можем решить проблему злоупотребления DNS на нескольких уровнях, и в ICANN мы совершенно очевидно концентрируем внимание на регистраторах и регистрациях, а также на контрактах и всем прочем, однако, чтобы решить проблему и снизить масштабы причиняемого ущерба, нам необходима

реакция всей системы в целом. Это… Поставщики услуг интернета и -электронной почты. Интернет-провайдеры. Сети передачи данных и список можно продолжать. Мы работаем в масштабной экосистеме и нам необходимо нечто, что поможет тем, кто пытается решить эту проблему, попасть в правильное место. Я здесь упоминал в общую -- следующий слайд. ICANN является нашим общим координатором, и мы говорим здесь о злоупотреблениях DNS. Мы оказываем определенное влияние, и Мэйсон совершенно правильно подчеркнул некоторые упреждающие действия. Меры по предотвращению являются ключевым элементом, потому что они поднимают планку, которую злоумышленникам приходится преодолевать, и усложняют причинение ущерба. Итак, ICANN для нас является общим координатором для этой группы заинтересованных сторон в этой среде. Однако у нас нет средства, покрывающего всю экосистему в целом в плане данных и всего прочего. Следующий слайд, пожалуйста. Что же мы можем сделать? Как представитель правоохранительных органов, я очень хорошо знаком с ICANN. У меня было множество плодотворных совещаний с группой регистраторов. Группа регистраторов и другие заинтересованные стороны, а также вы все можете использовать эти знания и направлять жалобы на злоупотребление в правильные инстанции. Однако не во всех правоохранительных органах или даже в сфере кибербезопасности ситуация в равной степени такая же. У нас

были комичные случаи, когда люди обращались в ICANN с требованиями приостановить регистрацию домена. ICANN этим не занимается. Иногда на самом деле неясно, куда направлять жалобы в зависимости от типа злоупотребления DNS. … данные или вредоносное ПО. Первым шагом не всегда является отмена регистрации доменного имени. Но это может быть правильным шагом, если в результате мы добьемся снижения ущерба, причиняемого пользователю интернета. Что произойдет, если мы не получим никакой реакции? В какие вышестоящие инстанции обращаться? И здесь все сводится к общему координатору. Куда нам обращаться дальше после требования к автору удалить опубликованный контент? Ничего не происходит. В какие вышестоящие инстанции обращаться? Регистратор не отвечает, время идет. Наличие всех этих механизмов – это следующий шаг, который мы можем предпринять, чтобы усилить барьер, и я считаю, что очень важно максимально усложнить жизнь злоумышленникам при причинении ущерба. Невозможно решить все проблемы только профилактическими мерами. К сожалению, всегда находятся обходные пути. У нас должна быть хорошая и эффективная система, чтобы мы могли предоставить быструю реакцию в течение обоснованного времени. Критически важными являются скорость реакции любого процесса и быстрые последующие меры. Я уже упоминал соглашения об общем доступе к данным. Важно, чтобы мы могли не только

постучаться в чью-то дверь и сказать «предоставьте нам IT-данные». Все должно проходить соответствующие проверки и получать нужный ответ, а соглашение об общем доступе к данным позволяют это реализовать. Надлежащим образом. И конечно, никому не хочется при решении вопроса впервые обращаться к регистраторам и регистратурам или разговаривать с автором проблемной публикации. На самом деле хотелось бы создать концепцию -- подготовить все технические моменты и реализовать соглашение, чтобы все знали процесс, какие проверки необходимы, как сказал Джефф в своем докладе ранее, чтобы вы знали, каким стандартам необходимо соответствовать, какие доказательства необходимо предоставлять. Это все очень-очень помогает при снижении ущерба и это все важные вещи, которые необходимо предоставлять сразу. Поэтому я считаю, что мы много чего можем сделать в плане эффективных профилактических мер. Но мы обсуждаем снижение ущерба, причиненного последствиями злоупотребления DNS. Снижение количества доменов не всегда обязательно приводит… злоумышленники эксплуатируют домены различными путями. Поэтому для того, чтобы остановить причинение ущерба, нам необходимо быть осведомленным не об этом. Теперь я хотел бы ответить вопросы.

ТОМАС РИКЕРТ: Большое спасибо, Крис. Я прочитаю один вопрос для вас от Максима. Есть ли у вас какие-либо планы по… в процессе? Любые злоупотребления в интернет проводятся через IP.

КРИС ЛЬЮИС-ЭВАНС (CHRIS LEWIS EVANS): Да, действительно это так и… сразу под регистратурой на графике. Прошу прощения, что все такое маленькое. Это было на предыдущем слайде. Поэтому да, они неопределенного представляют ключевую часть экосистемы. И да, я регулярно с ними общаюсь. У меня очень хорошие отношения с -- в их регионе, поэтому это важно. Спасибо.

ТОМАС РИКЕРТ: Еще один вопрос от Максима. Звучит множество призывов к упреждающему подходу. Существуют ли способы прогнозирования, если ничего плохого определенным доменом еще не происходило?

КРИС ЛЬЮИС-ЭВАНС: Очень сложно спрогнозировать будущее преступление. Это относится к разряду вещей, которые в реальности сделать нельзя. Но если у нас будут системы, готовые разобраться со злоупотреблениями сразу после их совершения, то это профилактическая мера, поэтому наличие правильной системы и способность быстро предпринять необходимые

действия – это очень эффективный шаг. Стороны, связанные договорными обязательствами, выполняют множество различных действий с данными в рамках концепции злоупотребления DNS и некоторые из них, возможно, -- я не имею полномочий обсуждать. Мы можем многое предупреждать, чтобы остановить злоупотребления, но, как вы и сказали, мы не можем прогнозировать их. Спасибо.

ТОМАС РИКЕРТ: Большое спасибо. Это область, которой нам также следует коснуться, когда мы будем обсуждать это с группой участников публичной дискуссии позже. Перед тем, как мы перейдем к последнему докладу, у меня есть один вопрос, если позволите. Вы упомянули на одном из ваших слайдов, что 85% случаев злоупотреблений имеют кибернетическую природу. Это все то, что мы называем злоупотреблениями DNS?

КРИС ЛЬЮИС-ЭВАНС: Нет, это не все злоупотребления DNS. Это включает СПАМ, что, собственно, зависит от вашего определения злоупотреблений DNS и это -- часть доклада Джеффа, определение злоупотреблений DNS. Поэтому да, это другой механизм, и также, поэтому я включил в доклад статистику ICO исключительно с целью дать понимание категорий злоупотреблений DNS.

ТОМАС РИКЕРТ: Спасибо, Крис. Я хотел продолжать, но вижу, есть вопрос от Моники. Я прочту этот вопрос как минимум потому, что это вопрос от женщины, поэтому давайте ответим на этот вопрос, прежде чем продолжить. Вопрос для Кристофера Льюиса-Эванса. Могли бы вы предоставить подробности по поводу тех 60% случаев утечки данных? Они произошли с помощью фишинга или вредоносного ПО? Можете ли вы также предоставить более подробные данные в отношении статистики и ее источников, и поясните, на основании чего вы относите утечку данных к фишингу или вредоносному ПО. Может, вы предоставите какие-то характерные признаки.

КРИС ЛЬЮИС-ЭВАНС: Эти данные опубликованы ICO. Это орган по защите данных в Объединенном королевстве. И чтобы сэкономить время, давайте я предоставлю детали в чате.

ТОМАС РИКЕРТ: Спасибо. Крис. Давайте перейдем к докладу последнему, но не менее важному. Докладчик Джеймс Блейдел из GoDaddy. Он будет говорить от имени стороны, связанной договорными обязательствами. Джеймс, вам слово.

ДЖЕЙМС БЛЕЙДЕЛ (JAMES BLADEL): Спасибо. Меня хорошо слышно?

ТОМАС РИКЕРТ: Да.

ДЖЕЙМС БЛЕЙДЕЛ: Отлично. Всем хорошего времени суток и спасибо, что пригласили меня на обсуждение. Одно из преимуществ выступать последними – это что я могу высказаться по некоторым пунктам и комментариям предыдущих выступающих, к тому же я внимательно слушал и записывал все в течение всей сессии. Мне очень хотелось представить точку зрения сторон, связанных договорными обязательствами, и вы увидите по мере презентации, что она во многом совпадает со всем тем, что было сказано до меня. Следующий слайд, пожалуйста. Итак, в целом, злоупотребления в -интернете, о чем сказал Томас во вступлении, – это проблема для нашей отрасли. И это приоритетная проблема для сторон, связанных договорными обязательствами. Мы видим, судя по всем усилиям касательно персонала и системы до сегодня, что эффективность, судя по цифрам, представленным Давидом, и цифрам в промежуточном отчете самых крупных сторон ICANN, что результат есть, и как злоупотребления в целом, так и злоупотребления DNS в частности, выявляются и устраняются в полном масштабе. Однако я считаю, что нам необходимо признать различие между злоупотреблениями в целом, злоупотреблениями данными и другими типами -- злоупотреблений в отличие от злоупотреблений DNS.

И это все относится к словам Томаса об ограниченном Уставом мандате ICANN в плане первоочередного внимания злоупотреблениям DNS.

Следующий слайд. На этом основании миссия ICANN, опять же, заключается в обеспечении безопасности и стабильности системы доменных имен. Но многие типы злоупотреблений, которые мы обсудили, в частности СПАМ, некоторые другие злонамеренные обманные действия в интер-нете сильно зависят от данных, и именно в этом месте мы начинаем уходить за рамки полномочий ICANN. Подобным образом ограничена и способность регистратур и регистраторов устранять злоупотребления и злонамеренный контент. Мы часто относимся к этому, как к крайней мере. Как у регистратуры или регистратора, у нас лишь один рычаг влияния. Это отмена или приостановка регистрации домена. Это не является приемлемым для таких злоупотреблений. Представьте, что мошеннические действия выполняются на странице в Facebook. Мы же не приостанавливаем регистрацию facebook.com. Если, например, на eBay продаются контрафактные товары, то приостановка регистрации eBay не является надлежащей мерой. Это касательно того, что мы называем крайней мерой. К счастью, множество регистратур и регистраторов находятся с другой стороны. Экосистема, например, GoDaddy включает регистратуру, регистратора и веб-сервер. Поэтому при обнаружении злоупотребления мы

располагаем большим количеством возможных мер. И именно это является одной из причин, почему стороны, связанные договорными обязательствами, заявляют, что лишь часть проблем злоупотреблений в интер-нете фактически подпадает под рамки полномочий ICANN. Однако в отрасли мы используем ряд других возможности за рамками ICANN, чтобы разбираться со злоупотреблениями различных типов. Следующий слайд, пожалуйста.

Итак, в сентябре прошлого года, как раз перед конференцией в Монреале -- около 10 регистратур и регистраторов ввели концепцию злоупотреблений DNS с целью реализации именно того, о чем говорили выступающие до меня, и установки стандартизированного определения злоупотребления. Определенные возможные стандартные действия. И, по-моему, Джефф упоминал отчет SSAC и говорил, куда именно следует подавать жалобы в зависимости от различных типов ситуаций, и каким может быть стандартная реакция по устранению злоупотребления.

С того времени собралось уже 50 организаций, подписавших эту концепцию, и Мэйсон говорил, что эта концепция многое меняет. Эта концепция смещает с рынка злонамеренные -- т.е. неэффективные или менее эффективные регистратуры и регистраторы. Она помогает в некоей мере создать общую способность отрасли устранять злоупотребления, расшатать

позиции организаций с наихудшими показателями и вытеснить их из отраслевого рынка. И как раз вчера все первоначальные и некоторые новые подписанты выпустили годовое обновление. Его можно найти на… dnsabuseframework.org и в нем поясняется, в чем заключается наш опыт касательно этой концепции, и некоторые тенденции в плане злоупотреблений. Поэтому вместо того, чтобы засыпать вас графиками и статистикой, приглашаю всех посетить этот сайт и ознакомиться с обновлением от каждого члена-подписанта этой концепции. Также в 2019 году немного ранее, кажется в апреле или в мае, Сеть политики и по вопросам Интернет и юрисдикции опубликовала технический документ White Paper, в котором подобным образом описаны все проблемы обнаружения и устранения злоупотреблений DNS, и все эти определения четко согласуются с концепцией злоупотреблений DNS, с той лишь разницей, что наша концепция включает веб-серверы. За пределами концепции злоупотреблений DNS, если говорить о данных, то имеются многочисленные отраслевые альянсы, ассоциации, коалиции и рабочие группы. Сюда входят совершенно разные организации, которые вам могут быть известны или неизвестны. Однако все они нацелены на борьбу с конкретными категориями злоупотреблений, например, СПАМ или жестокое обращение с детьми. Борьба с терроризмом. Финансирование набора кадров. Фармацевтика. Однако из-за того, что вы не видите конкретных действий и не знаете

категорий злоупотреблений согласно концепциям ICANN, это не означает, что ваша работа стоит на месте. По факту, множество сторон, связанных договорными обязательствами, также будут сотрудничать с другими организациями и, возможно, примут участие в других кампаниях. Следующий слайд, пожалуйста. Это текущее состояние дел. Посмотрите, в этом году ситуация часто менялась. Весь мир старался использовать интер-нет в основном как средство выживания в условиях пандемии, и мы говорим конкретно о пользователях из малого бизнеса. Все мы видели, как наши любимые рестораны меняют бизнес-модель на еду на вынос или уличную торговлю, чтобы выжить. Для тех из нас, у кого есть дети, мы все видим, что школы полностью изменяют форму обучения. Также и политические, гражданские и религиозные организации все больше смещаются в виртуальное поле из физического. То же самое справедливо и для ICANN. И я об этом говорю, потому что наша отрасль внесла определенный вклад в это смещение. В мире уже наблюдались эти тенденции, однако COVID-19 их ускорил на десятилетия и сжал этот переход до месяцев. И, конечно же, мы надеемся, что, когда это все закончится, мы будем немного более гибкими и сможем вернуться в традиционный режим.

Однако нам не следует удивляться, что преступники и мошенники, а также организации и оппортунисты также воспользуются этим переходом. Они также трансформируются и развивают свой подход. Их тактика следует за их жертвами,

а их жертвы больше не принимают участие в физической и в большей степени физической экономике. Преступники все больше исполь-зуют -- виртуальные и кибернетические возможности для атак, но с учетом всего сказанного данные не показывают, что это конец мира и интернета. Это далеко не так. Следующий слайд. Здесь мы возвращаемся к некоторым статистическим данным, предоставленным Давидом. В нашей отрасли наблюдалось несколько скачков в количестве заявлений о фишинге, и на одном из графиков Давида был представлен тренд. На графике было несколько точек, значение которых сильно отличалась от среднего по графику, и которые соответствовали нескольким пикам, наблюдавшимся весной, и паре пиков летом. Прежде всего, мы увидели небольшой рост, и я сейчас говорю более конкретно о GoDaddy, а не об отрасли в целом, так как у меня нет централизованной статистики. Мы видим рост приблизительно в 15%. Ничто не говорит ни о повышении показателей активности, ни о новых видах атак. Прямо сейчас в GoDaddy обрабатывается около 2000 заявок о фишинге в день. Это не касается доменных имен. Это не какие-то конкретные инциденты. Это просто заявки, и некоторые из них, должен заметить, приходят от панелей инструментов интернета, отправляющих множество дубликатов. Поэтому рассмотрение каждой отдельной заявки и удаление дубликатов требует много усилий. Также замечу, что из них около 8 или иногда

даже 3% являются решаемыми. Они либо больше не работают, либо у них не хватает ключевых элементов информации. Поэтому в этом плане очень много шума. Очень сложно найти конкретные и реальные инциденты и, возможно, на это мы могли бы смотреть операционно и -сотрудничать, возможно, с офисом технического директора и с организациями в отрасли, чтобы улучшить отсеивание несущественных заявок и сосредоточиться на реальных проблемах. Следующий слайд, пожалуйста. Небольшой пример. Не совсем относящийся к делу, но, я считаю, относящийся к тому же типу проблемы рассмотрения мошеннических кампаний, связанных с пандемией. Подобные заголовки преобладали в первой части года. Мэйсон упоминал скачки́, которые мы наблюдали в марте и апреле, когда почти все находились на более или менее полном карантине. Наиболее важно то, что эти были связаны, в первую очередь, с контентом. И это явление не особо новое. Все эти случаи преподносились в новой обертке, когда пытались привлечь максимум внимания или манипулировали страхами людей на ранних этапах пандемии. Но в сущности это был тот же старый фишинг и мошеннические атаки, с которыми мы боролись уже годами. Поэтому в нашем случае, например, в GoDaddy мы не считали, что нужно разрабатывать новые условия обслуживания, новые политики или пытаться создавать новая возможности. Мы увидели, что наш текущий набор средств срабатывает очень хорошо против

мошенничеств, связанных с COVID-19 в этом году, и в большинстве случаев устранение злоупотреблений происходило на уровне веб-серверов и не всегда это были атаки DNS. Должен подчеркнуть -- также были просьбы о комментариях Крису и Мэйсону в отношении превентивных и упреждающих мер, которые необходимо предпринять, -- мы получили множество предложений и на нас даже пытались давить политические деятели с требованиями заблокировать COVID во всей системе доменных имен. Блокировать регистрацию любых имен, содержащих определенный набор символов. Не позволяйте никому регистрировать домены, например, «коронавирус», они будут его использовать со злонамеренными целями, и это очень -- Я признаю привлекательность такого решения. Однако хочу подчеркнуть, что состояние вещей намного сложнее, чем может показаться не искушенному пользователю. Большинство вредоносных и злонамеренные доменных имен, встречавшихся нам до настоящего момента, вовсе не обязательно содержат слово COVID или coronavirus, поэтому подобный метод для них не сработал бы. Напротив, мы видели, что множество органов по охране здоровья и местные новостные организации и власти использовали доменные имена с этими словами для создания официальных сайтов с обновлениями и инструкциями. Поэтому нам необходимо подумать -- надеюсь, что профессионализм сообщества ICANN позволит нам

рассмотреть внимательнее такие призывы к блокированию определенных наборов символов в DNS в качестве решения конкретной проблемы. Это достаточно соблазнительное решение, но этот подход не обязательно эффективен и не обязательно имеет допустимый уровень ложных срабатываний или сопутствующего ущерба. Следующий слайд, пожалуйста. Это уже последний слайд. Самый важный вывод: злоупотребления необходимо учитывать. Мы не прячем проблему под коврик, но наша роль в ICANN и наша роль как регистратур и регистраторов, усиленная нашими договорными обязательствами с ICANN, достаточно ограничена. У нас имеются дополнительные средства, которыми мы можем воспользоваться. Мы считаем, что обсуждение этих тем в ICANN и дискуссии помогают получить более четкую перспективу от других членов сообщества, исследования OCTO и SSAC также очень важны, и сбор агрегированных данных по отрасли и широкая статистика тоже помогают. Но -- и я думаю это не сюрприз для всех нас. Вы увидите нерешительность сторон, связанных договорными обязательствами, в отношении начала разработки новой политики и внесение изменений в договоры в этой сфере. Во-первых, нам необходимо очень четко определить проблемы, например, чтобы это четко попадало под полномочия ICANN и, во-вторых, мы должны, -- кажется, это цитата Элиота, о которой говорил Мэйсон -- убедиться, что мы истратили все наши существующие

механизмы по договорным обязательствам, которые могли бы использовать в отношении небольшого количества недобросовестных организаций, регистрирующих все эти домены, и напротив, создали новую политику, которую можно или нельзя протестировать с этими проблемами, узнали бы, что есть определенные надежные методы, и как мы можем продвинуть этим методы, чтобы они были приняты и внедрены более широко. Это все мои слайды, Томас, спасибо, что пригласили меня. И спасибо, что выслушали.

ТОМАС РИКЕРТ: Большое спасибо, Джеймс. Джеймс, у нас есть один вопрос, адресованный вам. Это вопрос для Джеймса от Маркуса В. Будет ли развертывание проверенных надежных программ уведомления хорошим средством устранения любого шума, о котором вы упоминали?

ДЖЕЙМС БЛЕЙДЕЛ: Думаю, да. Надежные программы уведомления – это хороший способ отфильтровать ложные срабатывания и дубликаты заявок. Любые средства, которые помогут нашей команде и нашим командам сосредоточиться на реальных угрозах и снизить нагрузку, стоит поддерживать. Разумеется.

ТОМАС РИКЕРТ: Большое спасибо. У нас есть еще 17 минут времени. Я вижу, что в панели «вопрос-ответ» активно задаются вопросы и даются ответы от участников публичной дискуссии, и я хотел бы, чтобы так и продолжалось. Одно замечание, которое сделал Джефф Ньюман (Jeff Neumann). Он упомянул, что был вопрос касательно формата этих пленарных дискуссий, и их целью должны быть какие-то рекомендации или конкретные результаты. Мы все слушали презентации, но я не уверен, что все пришли к одному выводу, поэтому позвольте мне очертить несколько пунктов, о которых мы все можем согласиться и заявить, что мы получили нечто ощутимое, что можем представить, как результат обсуждения. Первое, о чем я хотел бы получить обратную связь от аудитории или участников публичной дискуссии, касается определения злоупотреблений DNS, потому что роли и действия, будь они проактивные и реактивные, всегда можно воспринять, как различные… зависят от этого. Об этом говорил в презентации Кристофер Льюис-Эванс и Джеймс Блейдел в своей презентации о концепции злоупотреблений DNS, и это коснулось пары пунктов о вредоносном ПО, ботнетах, фишинге, фарминге, СПАМе и некоторых моментов на тему СПАМа. Есть такая идея -- и это вопрос от Джеффа -- что вы и ваш отчет с SSAC, возможно, просто развили эту идею, потому что вы упомянули, что работали над определениями? Думаю, было бы очень хорошо для всех нас, если бы у нас было общее понимание о том, что именно

составляет проблему злоупотребления DNS, а что нет. Если у вас есть свои вопросы, пишите их в панели «вопрос-ответ». Также мне поступила рекомендация от персонала ICANN, что было бы лучше предоставить ограниченное время, чтобы мы не пытались включать звук каждого отдельного микрофона и высказываться, а я прослежу, что по мере наличия времени, ваши вопросы будут озвучиваться и на них будут даны ответы. Джефф, можете ответить на этот вопрос?

ДЖЕФФ БЕДЗЕР: Конечно, Томас, спасибо. Общей концепцией определения является механизм решения проблемы, потому что в этом случае, когда новый тип киберпреступления может не подходит под корневое определение, у нас есть возможность дать ему такое определение, охарактеризовать его с помощью параметров и направить в нужном направлении, поэтому я думаю, что это критический компонент для любого типа решения касательно злоупотреблений DNS, как общепринятого репозитория определений, к которому можно обратиться и определить вид и категорию конкретного случая мошенничества или злоупотребления домена.

ТОМАС РИКЕРТ: В SSAC рассматривали определение, предложенное в документе по концепции злоупотреблений DNS, в котором в основном развивается… работа над юрисдикцией?

ДЖЕФФ БЕДЗЕР: Спасибо, Томас. Да, эти 2 работы отдельно упоминаются в разделах, касающихся определений.

ТОМАС РИКЕРТ: Прекрасно. Хочет ли еще кто-то из участников публичной дискуссии высказаться -- не чтобы согласиться, а что бы что-то противопоставить, или -- можем ли мы воспринять молчание как знак согласия, что концепция злоупотреблений DNS – это хорошая начальная точка для общего определения злоупотреблений DNS? Я не имею в виду кого-то конкретного из участников публичной дискуссии, так как их у нас совершенно ограниченное количество. Включите свой микрофон и выскажитесь, если считаете что эти определения не совсем -- или им чего-то не хватает.

ДЖЕЙМС: Скажу пару слов. Я считаю, что это хорошее начало. Кажется, Джефф упоминал, что в отчете SSAC имеется призыв провести дополнительную работу по определениям. Кажется, тут есть несколько вопросов в чате на тему, куда нам двигаться дальше? Каков следующий шаг? И как нам надлежащим образом без повторов провести панельную дискуссию ICANN70, 71 и 72? Возможно, покинуть этот заколдованный круг можно, открыв- дискуссию в отношении определения, которая начнется с концепции на основании отчета SSAC,

и затем рассмотрит анализ, почему это приемлемо или неприемлемо для ICANN в виду ограниченной роли и механизмов, потом регистратуры и регистраторы должны рассмотреть это конкретное определение и -- я думаю, что это также и отчет SSAC -- Второй пункт – это найти ответственную сторону и способы передачи ответственной стороне, и, может быть, это предложение, с которого мы можем начать -- Я просто отвечаю на [неразборчиво] постоянно повторяющиеся вопросы в панели.

ТОМАС РИКЕРТ: Большое спасибо, Джеймс. Мэйсон, прошу вас.

МЭЙСОН КОУЛ: Я хотел дополнить, что сказал Джеймс. Я согласен с ним в целом -- концепция и отчет SSAC – это хорошее начало для разработки новых определений. Я просто хочу повторить, что я сказал в моей презентации. Я не хочу, чтобы мы погрязли или чрезмерного углубились в определения, тогда как злоупотребления будут продолжаться. Сейчас самое время предпринять действия по исправлению и не ожидать превентивных действий, параллельно пытаясь дать проблеме определение. Поэтому я хочу, чтобы в сообществе ясно понимали, что CSG и другие стороны, заинтересованы в этой проблеме, хотели бы увидеть, что в ICANN предпринимаются

определенные действия уже здесь. Микаэла уже упоминала, что мы можем постоянно встречаться и встречаться, и говорить о злоупотреблениях DNS, однако, нам необходимо предпринять какие-то конкретные шаги, поэтому, я надеюсь, мы не дойдем до точки, где погрязнем в определениях.

ТОМАС РИКЕРТ: Спасибо, Мейсон.

ДЖЕЙМС БЛЕЙДЕЛ: Может, это нормально, чтобы участники панельной дискуссии по нескольку раз отвечали на вопросы, а может и нет, я не знаю. Я думаю, что в этом месте есть некая точка расхождения для нас, и это звучит как «на старт, внимание, МАРШ!», и наличие определений и понимание этого, и у нас есть определенный круг полномочий. Это необходимо, чтобы предпринять следующие шаги. Я хотел бы подчеркнуть, потому что хочу убедиться -- может я не совсем в полной мере раскрыл тему, но работать нам необходимо. Они могут быть менее видимы в ICANN, потому что происходят в других местах и с другими заинтересованными странами и компаниями, но мы совсем необязательно застряли. Мы просто заняты делами в других местах.

МЭЙСОН КОУЛ: Спасибо за комментарий. Мне тоже не хотелось бы повторяться в панели, но я думаю, что есть эти недобросовестные от 8 до 10 организаций, о которых мы говорим уже многие месяцы. Может быть, имеются другие вопросы, происходящие в других местах, и которые решают стороны, связанные договорными обязательствами, мы этого не видим, однако, мне не хотелось бы прибегать к этому подходу AIM. Я хочу пользоваться надлежащим подходом к злоупотреблениям DNS, и я не вижу, что мы к этому приближаемся. Томас, возвращаю микрофон вам.

ТОМАС РИКЕРТ: Спасибо, Мейсон и Джеймс. Думаю, аудитория ожидает общения с участниками публичной дискуссии. Я очень рад этому. Думаю, никому не следует оправдываться работой по вопросам формирования политики и не предпринимать никаких действий. Вы знаете, по крайней мере, из моих обсуждений со сторонами, связанными договорными обязательствами, что многие из них -- все они, по крайней мере, те, кто здесь представлен, делают достаточно много. Но я уверен, что определения, тем не менее, критически важны и их необходимо сделать правильно. Мы должны убедиться, что регистратуры и регистраторы занимают свое место в экосистеме и могут предпринять необходимые действия согласно своим полномочиям. То же и с ICANN. Например, ассоциация ICO обрабатывает жалобы от общественности в основном по CASM, и Джеймс упоминал об этом в своих

комментариях и перед комиссией. Я связался с главой комиссии и спросил, при решении проблемы они более склонны обратиться к регистратурам и регистраторам или скорее к хостинговым компаниям, и они сказали, что предпочитают обращаться в компании по предоставлению хостинга, потому что хотят быть уверены, что незаконные материалы, которые во многих случаях имеют место в злоупотреблениях, более не распространяются из соответствующего источника. Поэтому я считаю, что нам необходимо это сделать правильно. Далее я хотел бы слегка коснуться несоответствий в статистиках. Некоторые говорят, что показатели сильно снижаются, другие говорят, что проблема не уменьшается, но, все остается более-менее на одном уровне. Давид, вы слышали, как участники дискуссии об этом говорили, и также давали комментарии в чате и в панели «вопрос-ответ». Могли бы вы пояснить разницу в различных высказываниях в разговорах о статистике?

ДАВИД КОНРАД: Я полагаю, что мы смотрим на разные части слона. Перед нами стоит вопрос, что на именно является злоупотреблением DNS. Что именно люди измеряют? Один из комментариев, который я дал в чате, был ответом на замечание, что определенные группы видят разные цифры, отличающееся от того что видим мы в наших наборах данных, и нам должно было быть интересно

увидеть наборы данных, которыми пользуются другие. Мы стараемся собрать как можно больше различных данных и предоставить эту информацию сообществу, чтобы помочь дать информационные основания подобным обсуждениям. И чем больше данных мы можем предоставить сообществу, тем, надеюсь, это приведет к более глубокому пониманию фактической реальности, стоящей за злоупотреблениями DNS в противоположность выдуманным историям. Поэтому с моей точки зрения данные, которыми мы располагаем, говорят о том, что со временем уровень злоупотреблений DNS снижается. Другие видят, что уровень злоупотреблений DNS повышается. И мне было бы интересно понять, в каких наборах данных люди видят эти результаты и эту статистику.

ДЖЕЙМС БЛЕЙДЕЛ: Томас, мне кажется, что это свидетельствует о неравномерном распределении проблемы в системе доменных имен и по интернету в целом. Я заметил это на слайдах Давида. На его графиках имеются аномальные точки, соответствующие определенным скачкам, и мне кажется, мы видели это в наших внутренних наборах данных. Это может быть тот случай, когда в целом уровень моря не повысился, но пару раз в год наступает прилив. Это не разная статистика, это не разные цифры, мы просто смотрим на проблему под разными углами и в разное время.

ТОМАС РИКЕРТ: Большое спасибо, Джеймс. Есть еще один вопрос для Криса. Когда я услышал от Джеймса и Давида, что было бы полезно собрать как можно больше статистики и данных, чтобы понять картину на основании разных источников и понять, где допущения, а где фактическая реальность, то вот вопрос: проводятся ли новые обсуждения в сообществах представителей правоохранительных органов для разработки отраслевого общего формата или определения, чтобы у нас была та же доказательная база, прошу прощения, наши чтобы наши политики соответствовали им?

КРИС ЛЬЮИС-ЭВАНС: Да, спасибо, Томас. Правоохранительные органы сделали большой шаг за последние несколько лет для повышения транспарентности касательно совершенных преступлений. Как они записываются? Какие фактические причины этих преступлений? Отчеты FEI IC3 красноречиво об этом свидетельствуют. Согласование этих данных в глобальных масштабах – это еще та задача. Мы достаточно много бьемся в ICANN над установкой стандартов записи данных, поэтому эту работу определенно необходимо довести до конца. Но мне кажется, что важнее предоставить данные и быть как можно более транспортными в том, к чему это ведет, и это позволит нам усилить сотрудничество и добиться результатов в масштабах экосистемы.

ТОМАС РИКЕРТ: Большое спасибо, Крис. У нас осталось 2 минуты, поэтому позвольте мне сделать вывод и подвести итог. Мы услышали несколько -- множество отличных комментариев. Думаю, есть общее мнение среди участников публичной дискуссии, но было бы хорошо иметь и определение проблемы. Что касается общей статистики или общих данных, думаю, стало ясно, что любые высказывания о большем или меньшем масштабе проблемы необходимо предоставлять с доказательствами из других источников данных, чтобы их можно было сопоставить с тем, что у нас есть. Запросы на другие действия приветствуются, это сильно помогло бы. Хотелось бы также вернуться к одному пункту, о котором упоминал Джефф в своей презентации. Это образование. Нам необходимы пользователи, которые… для фишинга или… других нехороших вещей, имеющих место быть. Это должна быть комбинация различных мероприятий по устранению недостатков, которые могут быть предприняты различными участниками системы с соответствующими ролями, сторонами с договорными обязательствами ICANN, правоохранительными органами и другими. Но если бы мы могли поработать над ними, то это было бы хорошее начало. Я не принимаю участия в создании документа концепции по злоупотреблению DNS, но многие ожидают этот документ. Поэтому, как рекомендация, в этом документе должна содержаться база для обсуждения разных понятий, таких как определения для систем проверенных

программ-уведомителей и пр. Нам не нужно -изобретать колесо, но нужно продолжить предыдущую работу. И наконец, хочу поблагодарить участников дискуссии. Я хотел бы поблагодарить персонал ICANN и, в частности, техническую команду за то, что сессия прошла гладко без технических проблем. Я хотел бы поблагодарить всех вас… Очень сложно целые часы проводить в удаленных конференциях без личных встреч с людьми на кофе-брейках, поэтому спасибо, что вы с нами. Спасибо за внимание. На этом еще раз всех поблагодарить. Совещание закрыто.

[КОНЕЦ СТЕНОГРАММЫ]