САН-ХУАН - GAC: заседание с PSWG
Вторник, 13 марта 2018 г. - с 08:30 до 09:30 AST
ICANN61 | Сан-Хуан, Пуэрто-Рико

CATHRIN BAUER BULST: Хорошо. Доброе утро, всем.И большое спасибо за то, что вы присоединились к нам здесь, в этом большом зале вместо того, чтобы наслаждаться карибским солнцем после прекрасного торжества. Мы высоко ценим вашу преданность Рабочей группе по общественной безопасности, так что это официальное заседание Правительственного Консультативного Комитета и Рабочей группы по общественной безопасности. Меня зовут Катрин Бауэр-Булст (Cathrin Bauer-Bulst). Я являюсь одним из двух сопредседателей этой рабочей группы, и здесь я нахожусь с моим сопредседателем Лорин Капин (Laureen Kapin). Итак, у нас есть два основных пункта повестки дня, и мы будем говорить о рабочем плане рабочей группы по общественной безопасности, а затем о работе OCTO и инструмента DAAR, и мы собираемся начать с Рабочего плана, но сначала я позволю остальным представителям Рабочей группы по общественной безопасности сказать вам доброе утро.

НЕИЗВЕСТНЫЙ ОРАТОР: Доброе утро, я Лорин Капин (Laureen Kapin) из Федеральной торговой комиссии Соединенных Штатов, я занимаюсь защитой интересов потребителей, в первую очередь, и бладарю всех людей, присоединившихся к нам на самой первой сессии сегодня, хотя она и начинается в 8:30, ождидайте продоллжения встреч.После этой сессии мы фактически переключимся на другие темы и будем фокусироваться на системе WHOIS, и на GDPR, поэтому сегодня утром вы получаете большую дозу информации от нас, и, надеюсь, это будет, надеюсь, это будет, по крайней мере, приятной и интересной дегустацией.

IRANGA KAHANGAMA: Привет, доброе утро.Иранга Кахангама (Iranga Kahangama) от Федерального бюро расследований США. Я хотел еще раз поблагодарить вас за посещение. Что касается темы, то я работаю над проблемами злоупотребления DNS, которые относятся к DAAR, где у нас есть некоторые из сотрудников ОСТО, и я приглашаю вас посмотреть на слайды и подумать о том, как через политику или другие рекомендации мы можем поддержать инициативу. Это было бы полезно для безопасности интернет-сообщества. Я с нетерпением жду возможности пообщаться с вами по рабочему плану. Благодарю.

CATHRIN BAUER BULST: Большое спасибо.Итак, мы начнем, да.На самом деле, это было бы. Итак, Лорин просто сделала хорошее предложение, чтобы те из вас, кто является членом Рабочей группы по общественной безопасности, чтобы вы просто подняли руку, чтобы вас увидели люди, потому что у нас много людей в аудитории, которым может быть интересна наша работа и которым, может быть, будет интересно побеседовать с одним из нас в течение дня. Поэтому могу ли я попросить членов Рабочей группы по общественной безопасности лишь ненадолго поднять руки, чтобы каждый мог увидеть, где они находятся.

LAUREEN KAPIN: Вот эти люди, если у вас есть вопросы, то не только к нам на сцене.У нас много членов. И они все рады общаться и отвечать на вопросы.

CATHRIN BAUER BULST: Вы знаете, что с воскресной сессии мы собираемся принять рабочий план Рабочей группы по общественной безопасности на предстоящий период.Мы на высоком уровне в воскресенье это обсудили, и мы хотим воспользоваться шансом сейчас, возможностью теперь ознакомить вас с ним еще раз и посмотреть, есть ли какие-либо окончательные комментарии по этому вопросу, прежде чем он будет принят в коммюнике

GAC в конце этой конференции.Первая цель связана с вопросом злоупотреблений, и Иранга занимается данной темой и представит ее нам сейчас.

IRANGA KAHANGAMA: Спасибо.Так, как я уже упоминал, это один из наших основных планов работы, цель которого состоит в том, чтобы ICANN находилась в более выгодное положение в плане устранения злоупотреблений DNS.Есть ряд сообществ, которые определили это как высокий приоритет. Есть несколько отчетов, в которые составили команды, и мы хотим продолжать двигаться вперед. Чтобы ... поскольку я упомянул проект отчетности о деятельности по злоупотреблению доменами, о котором вы еще услышите позже, это большой рабочий план для нас. И тогда для тех, кто заинтересован, есть также индекс состояния рынка gTLD и индекс состояния технологии идентификатора, две отдельные программы, связанные с инициативой ICANN в области открытых данных, которая пытается добавить больше данных и чисел к некоторым злоупотреблениям, состоянию на макро- и микроуровне, чтобы мы были в лучшем положении, чтобы сообщить об этом злоупотреблении, поэтому пропущу пару пунктов, я думаю, что все это говорит о том, что, и вы можете оставить это, мы движемся к созданию принципов.Мы считаем, что общие механизмы базового понимания должны

быть приняты всеми частями сообщества, и мы можем договориться и зафиксировать это, как только мы сможем согласовать их в группе. И затем, с точки зрения новой работы, я думаю, что еще одно сообщество, которое мы еще полностью не задействовали, - это SSAC, и мы слышали, что они запускают ряд интересных инициатив, и мы хотели бы более формально участвовать в них. Поэтому я думаю, что на этой конференции завтра состоится заседание в 15:15, которое будет открытым собранием SSAC, о котором они упоминали, и все свободно его могут посетить, и, возможно, будет интересно принять в нем участие и увидеть некоторые из элементов безопасности, над которыми они работают. Они заинтересованы в регистрационных услугах и технических аспектах этого, что, конечно, очень интересно, учитывая некоторые соображения с GDPR. И поэтому я думаю, что есть ряд людей, ориентированных на безопасность, поэтому в плане охвата мы попытаемся более формально установить отношения с ними, чтобы у нас был лучший механизм обратной связи. Так что это основной обзор того, чего мы пытаемся достичь. Я приветствую любого, у кого есть идеи. Мы, конечно, открыты. Существует множество проблем с безопасностью в Интернете и DNS, поэтому мы ограничены в ширине полосы, но я думаю, что мы преуспеваем, и мы обязательно будем информировать вас по мере развития событий. Я думаю, что для этой встречи этот

вопрос ушел на второй план, потому что вопросы GDPR больше привлекают наше внимание, но мы должны оставить это как высокий приоритет. Благодарю.

CATHRIN BAUER BULST: Поэтому позвольте мне напомнить членам GAC, что у вас также есть копия этого рабочего плана, прикрепленная к вашему инструктивному материалу для пункта 11 повестки дня, потому что мы представили его вам снова в воскресенье, поэтому на всякий случай, если вы хотите прокрутить в своем собственном темпе и на досуге, именно там вы можете его найти.

LAUREEN KAPIN: Итак, вкратце о мерах защиты потребителей. На самом деле, этой проблеме уделяла основное внимание группа по анализу потребительского доверия, выбора потребителей и конкуренции, и я возглавляла подгруппу, которая занималась мерами защиты, но, в принципе, эта тема является продолжением нашей существующей работы, а именно проведение политики по защите общественности онлайн.Это своего рода главная цель этой части плана работы, поэтому мы участвуем в соответствующих обзорах. Мы сотрудничаем с различными подразделениями организации ICANN, в частности с соблюдением и безопасностью, а также

поддерживаем связь с сообществом, чтобы говорить о проблемах, потому что все заинтересованы в том, чтобы обеспечить безопасность онлайн-сети для пользователей и вдохновлять доверие потребителей, чтобы они продолжали пользоваться интернетом. Таким образом, в этой связи есть много разных заинтересованных сторон и рабочих потоков, и это включает в себя новый PDP по анализу последующих процедур , мы также помогаем внедрить систему аккредитации служб конфиденциальности и регистрации через доверенных лиц, так что есть много разных рабочих потоков, которые будут продолжать работать в этом направлении.

CATHRIN BAUER BULST: Хорошо.Я возьму следующие 2 пункта на следующей странице по подотчетности и предотвращению злоупотребления DNS, так что в связи с подотчетностью, мы на самом деле все еще ищем ответственного, который взял бы на себя эту тему. И эта тема еще не закрыта для Рабочей группы по общественной безопасности. Существует ряд рабочих потоков, связанных с общественной безопасностью, которые имеют отношение к политической стороне, чтобы быть более эффективными в предотвращении некоторых из них, и эта работа включала в себя, где может быть ожидание от пользователей, что это безопасное пространство для детей, и меры защиты, которые

были приняты в Пекинском коммюнике необходимо оценивать с точки зрения эффективности с целью возможной адаптации их в любых последующих раундах, и в рабочем потоке ведется и другой тип работы. Я не буду вдаваться в подробности здесь, но, пожалуйста, поговорите со мной или итальянской командой GAC об этих усилиях. Я остановлюсь здесь и посмотрю, есть ли у кого-нибудь комментарии по первой стратегической цели. Давайте перейдем ко второй стратегической цели, которая сосредоточена на RDS, в частности, и одним из основных пунктов здесь является WHOIS и доступ к регистрационным данным GDPR, итак, Лорин.

LAUREEN KAPIN: Я приторможу это, как мы говорим, потому что мы подробно обсудим эту тему сразу после перерыва на кофе, поэтому вам просто нужно знать, что система WHOIS и все преимущества и обязанности, которые с ней связаны, являются частью нашего рабочего потока, и на этом действительно была сосредоточена наша более поздняя работа.

CATHRIN BAUER BULST: Это приводит нас к PDP по следующему поколению RDS.Грег, Вы хотите сказать об этом пару слов? Нет? Хорошо. Я так думаю.

НЕИЗВЕСТНЫЙ ОРАТОР: Продолжается.

CATHRIN BAUER BULST: Продолжается, да.Затем у нас ведется работа по точности регистрационных данных, которая, как вы знаете, продолжается уже долгое время, в настоящее время проводится проверка точного синтаксиса записей регистрационных данных. Сообщество еще фактически не рассмотрело вопрос проверки личных данных владельцев регистраций, и все еще есть много возможностей в плане общественной безопасности, чтобы повысить качество регистрационных данных GDPR, и мы видим некоторые многообещающие инициативы также в мире ccTLD, как это можно сделать надежным, но недорогостоящим образом, и я думаю, что мы продолжим наши усилия, чтобы посмотреть, как эти усилия могут масштабироваться и передаваться в мир gTLD.

IRANGA KAHANGAMA: Я думаю, что это важный раздел рабочего плана, и потому люди не должны забывать о том, что GDPR требует точности данных, а также часть ответственность связана с необходимостью иметь данные, поэтому я думаю, что мы не сосредотачивали слишком много внимания на это, потому что

в данный моментс мы просто пытаемся сохранить данные или поддерживать доступ, но мы не достигли этого второго, а именно убедиться, что данные на самом деле точны, и поэтому я думаю, что по мере продвижения вперед, это ... это производительность по отношению к этому ключевому инструменту, и эта группа по обзору RDS, в которую GAC назначил из СШАЛили ... из Интерпола и меня. Этот обзор в настоящее время продолжается и все еще находится на ранних стадиях, и мы сообщим вам о его усилиях, возможно, на следующей конференции ICANN в Панаме. Итак, еще один повод, чтобы поехать на следующую конференцию.

LAUREEN KAPIN: Это наша стратегическая цель номер два.Есть ли у кого-нибудь какие-либо вопросы или замечания по этому поводу? Хорошо. Тогда мы перейдем к стратегической цели 3, это своего рода фундамент. Основополагающая стратегическая цель. Обеспечение эффективной и отказоустойчивой работы PSWG, поэтому это действительно фокусируется на нашей организационной структуре и наших процедурах. Таким образом, вы увидите, что разработка рабочего плана - это первое. Укрепление руководства. Удостовериться, что, как мы уже упоминали в воскресенье, мы хотим иметь надежный тыл, чтобы у нас были люди, которые могли бы сосредоточиться на многих

важных темах, которые развиваются в рамках усилий по разработке политики и информировании заинтересованных сторон. Мы хотим укрепить членство. Попадает под категорию повышения приверженности. Одна из идей, которые мы обсуждали с руководством GAC, заключается в том, чтобы призвать членов GAC рассмотреть вопрос о выдвижении кандидатур и действительно обратиться к правоохранительным органам и ... в каждой стране есть сотрудники правоохранительных органов и люди, достаточно осведомленные в сфере расследований и в сдерживании преступной деятельности. В частности, поскольку DNS задействована, и мы знаем, что эти проблемы становятся техническими и сложными, и у вас есть эксперты в вашей стране, с которыми вы можете консультироваться, и мы будем призывать вас делать это формально и обращаться к этим людям, и еще лучше, назначить их в качестве советников Рабочей группы по общественной безопасности. Попросите их присоединиться к нашему списку электронной почты. Приходить на собрания, если они являются ресурсами для этого. Таким образом, действительно важный момент состоит в том, как мы действительно вовлечем всех в эти очень важные проблемы общественной безопасности, поэтому я хотела бы подчеркнуть это, и, конечно же, мы являемся рабочей группой Правительственного Консультативного комитета, поэтому мы хотим обеспечить

постоянную связь с GAC и с руководством GAC, то есть, вы знаете, работать и информировать вас, когда появляются горячие темы, требующие быстрых действий, и мы можем дать отличный пример для иллюстрации этого, который имел место совсем недавно, когда, вы знаете, мы попросили вас посмотреть на сложные вопросы и проанализировать их, и это не идеальная ситуация, но, к сожалению, у нас сложилась такая ситуация, и мы хотим убедиться, что мы делаем все максимально эффективным образом, чтобы предупреждать вас и дать вам возможность ознакомиться с важной работой PSWG, чтобы мы могли получить ваш вклад и одобрение, и чтобы мы могли работать с вами, чтобы убедиться, что продукт отражает консенсусную позицию GAC, так что это также фигурирует в нашем рабочем плане, и в этой связи мы всегда с очень большим нетерпением желаем услышать от вас о том, что мы делаем хорошо и что мы можем делать лучше. Поэтому, пожалуйста, не стесняйтесь. Как вы можете видеть, мы не особенно застенчивы, и мы рады поговорить с вами в коридоре или по телефону. В любое время, если вы считаете, что необходимо внести какие-то корректировки. Итак, это стратегическая цель 3 нашего рабочего плана, и я рада попросить вас задать вопросы или комментарии. Джейсон.

КАНАДА: Я Джейсон, член Рабочей группы по общественной безопасности из Канады. В Абу-Даби было отмечено, что мы довольно смешанная группа: много людей из Северной Америки и много из Европы, но и мы хотели бы разнообразить свое членство, и если у вас есть люди, которые, по вашему мнению, будут подходящими кандидатами для работы в Рабочей группе по общественной безопасности, пожалуйста, обращайтесь к нам, и мы можем рассказать вам, как принять участие. Чем разнообразнее мы будем, тем сильнее будут идеи, которые мы будем передавать, возможно, и так как многие из нас из Северной Америки или Западной Европы, мы хотели бы представлять точки зрения со всего мира, а не только наших соответствующих государств, поэтому, пожалуйста, обращайтесь к нам, и мы можем, безусловно, помочь вам принять участие или помочь кому-то из ваших представителей правоохранительных органов заниматься темой общественной безопасности. Спасибо.

CATHRIN BAUER BULST: Большое Вам спасибо, Джейсон за то, что Вы отметили этот очень важный момент.Это Катрин. И я просто хочу добавить, что разнообразнее будет наш состав, тем лучше мы будем отражать полный GAC, так что это очень важно для нас, поскольку мы работаем, как ваша рабочая группа, чтобы помочь вам в вашей работе, и мы можем сделать это лучше,

если мы отразим различные позиции GAC также и в группе. И просто скажу, что наша работа на самом деле не ведется только на этих встречах. У нас проводятся ежемесячные телефонные звонки со всем составом Рабочей группы. Мы организуем еженедельные телефонные звонки с руководством и членами, и не имеет значения, откуда вы подключаетесь. Это обычный зал Adobe. Но если вы хотите назначить эксперта Н, который не сможет принимать участие, это важно. Лучше, если вы сможете встречаться с людьми лицом к лицу время от времени, но большая часть работы, которую мы делаем, по существу происходит за пределами встреч через дистанционное участие, поэтому я хотел бы заверить всех вас, кто обеспокоен вопросом ресурсов и инвестирования в работу Рабочей группы по общественной безопасности, что это не должно препятствовать участию. Поэтому я просто остановлюсь здесь и посмотрю, есть ли какие-либо дальнейшие комментарии к пункту 3? Или, если кто-то настолько полон энтузиазма, то может просто вскочить и присоединиться.

[Смех]

Просто шучу. Если нет никаких дальнейших комментариев, мы перейдем к стратегической цели 4 о работе по информированию с другими частями сообщества и заинтересованными сторонами за пределами этой среды.Так

что речь идет об оценке того, что мы делаем в нашем рабочем плане.Итак, одним из ключевых моментов является обеспечение того, чтобы при определении наших приоритетов мы устанавливали правильные приоритеты, и, конечно же, для этого нам нужно поговорить со всеми, кто присутствует в зале, а также и с людьми за пределами этого зала, чтобы выяснить, что влияет на них с точки зрения проводимой здесь политики, как они оценивают работу над текущей политикой, и где есть возможности для улучшения или даже большие проблемы, о которых Рабочая группа по общественной безопасности, по их мнению, должна проинформировать GAC или же предоставлять экспертные материалы. Мы также работаем над тем, чтобы повысить информированность Рабочей группы по вопросам общественной безопасности через другие правительственные учреждения, чтобы убедиться, что существует горизонтальная координация и страны знают о возможности обеспечить ... Рабочей группе по общественной безопасности, потому что, конечно, речь идет не только о полиции. Существует много вопросов общественной безопасности, за которые Рабочая группа по общественной безопасности официально отвечает и которые необходимо полностью отразить в нашей работе. И затем мы работаем над снижением барьеров для участия. Также путем предоставления более полной информации. Я имею в виду, что вы, вероятно, все были

хорошо знакомы с этим к тому моменту, когда я объяснил, что происходит в ICANN, люди либо крепко спят, либо вы знаете, что час, который у меня есть для моей встречи, уже закончился.

[Смех]

Так что действительно сложно получить нужный вклад, потому что, когда люди возвращаются, и они, знаете ли, интересуются: что вы решили на этой встрече? Что мы делаем по этому вопросу? На самом деле, мы просто побеседовали, и работа идет, но это занимает некоторое время. Из-за этого по многим причинам очень сложно или может быть очень сложно сделать так, чтобы люди были достаточно осведомленными о том, что происходит здесь и почему это важно, а также поставить их в положение, когда они могут определить, почему это важно для них и как они могут внести свой вклад. И мы работаем над тем, чтобы, в принципе, снизить эти барьеры. С помощью информационных бюллетеней. Кратко о том, что происходит здесь, чтобы сделать нашу работу доступной для тех, кто не занимается вопросами управления Интернетом на ежедневной основе, и мы получили очень хорошие результаты в ходе нашего межсессионного совещания, в частности, по этим вопросам, так как там были представлены многие учреждения, которые обычно не участвуют в этой работе и которые задали очень

много хороших вопросов о том, почему мы делаем определенные вещи и как мы их делаем, и у кого были хорошие идеи о том, что нам нужно сделать, чтобы их лучше информировать, так что мы работаем над реализацией этих идей. И, как вы можете видеть здесь, есть еще больше возможностей для добровольцев прийти и присоединиться к нашим усилиям. Я чувствую, как будто мы на мероприятии по сбору средств.

[Смех]

Так…

LAUREEN KAPIN: И Иранга расскажет об усилиях по информированию, которые мы провели во время этой конференции.

IRANGA KAHANGAMA: Спасибо, да, возможно, это подходящее место, чтобы просто снова кратко упомянуть, что мы хотели попробовать поговорить с SSAC.Они упомянули, что они изучают интересные вещи, и в ходе информационно-пропагандистской работы мы беседовали с регистратурами и регистраторами о некоторых проблемах RDS, с WHOIS, просто пытаясь получить информацию о том, как они видят все это. Таким образом, это были два вида деятельности по информированию, которые мы реализовали. OCTO, конечно,

мы будем говорить о них через несколько минут, когда мы будем говорить о DAAR, и мы открыты, и я думаю, что в этом есть много творчества, поэтому, если вы думаете, что у кого-то есть другие идеи ... мы бы хотели исследовать это.

CATHRIN BAUER BULST: Спасибо, и с точки зрения лучшего знакомства с нашими частями сообщества, я хочу напомнить всем об общественном мероприятии с регистраторами сегодня вечером.Я думаю, что оно начинается в 6:30 на террасе. Поэтому, пожалуйста, присоединяйтесь к нам. Если вы также хотите принять участие в лучшем ознакомлении с другими частями сообщества. И я думаю, что на этом мы завершаем, хорошо, я остановлюсь на минуту и посмотрю, есть ли другие креативные идеи по пункту 4?И если нет, на этом мы завершаем обзор планов работы. Если у вас есть другие комментарии или вопросы или предложения или изменения по рабочему плану, я попрошу вас либо обратиться к одному из нас, либо отправить нам электронное письмо к концу дня сегодня, и в противном случае мы будем считать этот вопрос закрытым, и мы предложим формулировку для коммюнике GAC, чтобы принять настоящий план работы. Хорошо. Итак, мы все настроены на это? И это означает, что мы можем перейти ко второму вопросу нашего засденаия, которым является беседа с OCTO и DAAR, о, отлично, я вижу, что Дэвид

подтягивается.Дэвид благодарим Вас за то, что Вы нашли время и делаете это, несмотря на то, что, как я понимаю, Вы сильно простыли.

DAVID CONRAD: Доброе утро, извиняюсь за хриплый голос, и я, возможно, буду кашлять время от времени, но я подменяю Джона, который, похоже, хорошо провел время на вчерашней вечеринке.

[Смех]

И это не результат вчерашней вечеринки, благодарю. Переходим к следующему слайду. Итак, я уверен, что большинство из вас знакомо с тем, что такое DAAR. Для тех из вас, кто не знает, DAAR - это система отчетности, которую мы разрабатываем с помощью кибергруппы iThreat для отслеживания злоупотреблений, которые мы видим, как было определено GAC в Пекинском коммюнике. MODULO, что мы не видим с нашей высоты в ICANN.Также как спам. Чем же DAAR отличается от множества других инструментов отчетности? В принципе, он отличается объемом данных, которые мы собираем.Мы фактически собрали целую кучу данных. С течением времени собираются данные, которые мы, на самом деле, планируем хранить для проведения исторических исследований. И основное внимание уделяется

множеству злоупотреблений, с тем чтобы мы могли генерировать информацию, которая является прозрачной и воспроизводимой для содействия коммуникации, для содействия разработке политики в сообществах ICANN. Следующий слайд, пожалуйста. Я уже говорил об этом. Таким образом, одна проблема заключается в том, что мы лицензируем значительную часть данных, которые мы используем для DAAR, и что данные могут быть или не быть доступными. Следующий слайд. Итак, для чего можно использовать DAAR? Таким образом, очевидно, что основной задачей является отчет об активности угроз на уровне верхнего уровня или уровне регистратора. Ее можно использовать для изучения истории угроз безопасности или деятельности по регистрации доменных имен. Это может помочь операторам регистратуры и регистраторам и резервным операторам регистратуры в понимании или анализе того, как управлять своей репутацией в системах борьбы со злоупотреблениями.Репутационные списки и такого рода вещи. Это позволяет нам изучать поведение, связанное со злонамеренной регистрацией, и нацелено на оказание помощи в обеспечении оперативной безопасности в сообществах.Мы используем зонирование TLD, которое собирает все данные для аналитики регистратуры gTLD. Речь идет фактически об использовании централизованной службы данных зоны, и, где возможно, мы осуществляем трансфер

зоны. DAAR будет использовать только имена, появляющиеся в зонах. Мы не пытаемся заглянуть в базы данных регистратуры или регистратора до того, как эти имена будут выгружены в зоны. В настоящее время у нас около 1240 gTLD, что составляет примерно 195 миллионов доменов. К нам обратились ряд ccTLD, которые желают участвовать в DAAR, и мы работаем над их включением в систему DAAR. DAAR также использует WHOIS. Мы используем ее небольшую часть. В первую очередь, регистратора, но даже это оказывается довольно проблематичным. Поскольку DAAR нацелена на потенциальной разработке системы, которая может быть воспроизводима кем угодно, мы не используем любую информацию, которая доступна внутри ICANN, и только внутри ICANN. Фактически мы используем информацию, доступную общественности, так или иначе. В результате этого, вы знаете, мы пытаемся извлечь информацию из миллионов доменов через существующие серверы WHOIS, и многие из вас знают, что ограничение допустимой частоты запросов может быть немного сложной задачей. Следующий слайд, если посмотрим на группы данных об угрозах, мы используем многие из них. Мы пытаемся создать уникальные данные FI, чтобы у нас не было ложных, так много ложных срабатываний.Мы используем несколько групп данных о злоупотреблиниях доменами или URL-адресами, генерирующих ежедневные подсчеты доменов, связанных с

фишинговым дном Интернета и спамом. Мы вычисляем фото ASL и кумулятивные области злоупотреблений и создаем гистограммы, графики дней живого использования. DAAR нацелена на то, чтобы отразить, как люди, не входящие в ICANN и сообщество ICANN, видят экосистему доменных имен. Следующий слайд. Следующий слайд. Мы в OCTO или ICANN не составляем собственный список блокировок. Это не наша работа. И я сомневаюсь, что мы сможем это сделать хорошо. Мы представляем совокупность данных, доступных через внешние стороны, и именно эти стороны генерируют эти списки, чтобы фактически блокировать угрозы. DAAR собирает те же данные о злоупотреблениях, о которых сообщают в отрасли, поэтому мы не генерируем ничего нового здесь. Одна из распространенных проблем, с которыми сталкиваются люди, заключается в том, что мы генерируем новые данные, которые могут быть неточными, и мы неоднократно повторяли, что это то, что интернет-провайдеры, почтовые операторы используют в повседневной работе. Здесь мы ничего нового не делаем. Следующий слайд. Критерии включения одного из этих репрезентативных списков блокировок в систему DAAR. Они должны обеспечить классификацию угроз, которая соответствует группе угроз, на которые мы смотрим. Сообщества оперативной безопасности должны доверять RBL за точность и ясность процесса. Они должны иметь

позитивные отклики в научной литературе, и RBL должен быть широко принят и принят во всех сообществах оперативной безопасности. И это демонстрируется обычно тем, что каналы включены в коммерческую деятельность по безопасности, а продукты, они используются сетевыми операторами для защиты своих пользователей и устройств, и они защищены или используются почтовыми провайдерами для защиты от спама и других атак. Следующий слайд.RBL, которые мы используем, вездесущи. Они, как правило, блокируют не только просто нежелательную коммерческую электронную почту. Они используются в браузерах, например, Google Chrome использует список APWG. Они используются в облачной и контентной сервисной системе ... их использует SERBL и Amazon. WAF, я забыл, что означает WAF, использует RBL для блокирования злоупотреблений в объемных атаках, а Google блокирует вредоносный URL-адрес и мошенничество с рекламными словами.RBL используются в DNS через так называемые зоны политики ресурсов, визуально развитые, но в настоящее время используются в нескольких резольверах и спам, WHOIS и другие предоставляют эти RBL, используя формат RPZ, связанный больше с тем, как используются резольверы, поэтому мы не рискуем здесь, не используем материал, который является экспериментальным. Это материал, который фактически используется в производственных услугах, а также в коммерческих

продуктах. Следующий слайд. Мы также обращались в академические круги, чтобы проанализировать эти RPL, чтобы убедиться, что они используют лучшие практики и используются таким образом, чтобы исследователи могли доверять, и это список ряда академических отчетов, в которых используются RBL, которые мы используем в DAAR. Следующий слайд. Таким образом, текущий набор RBL, который мы используем, является только списком доменов SERBL. Список SPAM блокировов доменов . Рабочий список борьбы с фишингом. Патруль вредоносного ПО, который представляет собой составной список всех тех, кого вы видите справа, трекер фишинга, трекер программ-вымогателей и трекер THEODO. Следующий слайд. DAAR не идентифицирует все злоупотребления. Нет надежного провайдера, который бы мог видеть все злоупотребления. У каждого свой взгляд на интернет-злоупотребление, а разные RBL сосредоточены на конкретных вещах. Таким образом, одна из причин, почему мы объединяем эти RBL, это чтобы попытаться получить более сложное представление об Интернете. Следующий слайд. Нам часто задают вопрос, почему мы сообщаем о спам- доменах.Таким образом, в Хайдерабадском коммюнике была выражена заинтересованность GAC в информации о спаме. И, с нашей точки зрения, большая часть спама отправляется с помощью незаконных или дублирующих средств, которыми обычно

являются ботнеты. Его уже не связывают только с контентом по электронной почте, есть спам-ссылки. Есть спам-твиты. Даже в Фейсбуке есть спам и других системах обмена сообщениями. Спам, на самом деле, является основным средством доставки большинства других угроз безопасности. Тех, что GAC упомянул в своем Пекинском коммюнике. Можно рассматривать спам как своего рода облачный сервис, лавинный ботнет, который предоставляет пользователям регистрацию доменных имен, чтобы фактически способствовать передаче спама. Мы в DAAR находили доменные имена в самом тексте спам-сообщений. Это то, что люди нажимают, тем самым запуская загрузку вредоносного ПО или что-то подобное. Самое главное, объем спам-доменов влияет на то, как широко или агрессивно администраторы безопасности или электронной почты применяют фильтрацию. Обычно вы обнаружите, что системные администраторы в первую очередь делают акцент на спам, потому что это очень хороший индикатор скомпрометированных доменов. Следующий слайд, пожалуйста. Следующий слайд. Так что сейчас система DAAR находится в производстве. Мы используем ее внутренне уже в течение некоторого времени. Мы не начали публиковать отчеты, которые генерирует DAAR, потому что мы хотим делать все правильно, а не быстро, поэтому то, что мы фактически установили, - это независимый сторонний обзор

методологии, которую мы используем в DAAR для сбора данных.И эти обзоры, на самом деле, закончились только вчера. Второй - через пару дней. Мы собираемся просто передать эти отчеты сообществу, если по отчетам будут внесены какие-либо предложения об изменениях, мы, конечно, внесем эти изменения. Мы намерены провести эти обзоры и предоставить их в SSAC, и попросить SSAC выразить свое мнение о том, что мы должны делать с методологией, которую использует DAAR, но на данном этапе внутренние отчеты и графики, которые вы увидите, в настоящее время являются только внутренними. Они должны быть доступны. Наша цель на данном этапе - сделать этот материал доступным для сообщества для обсуждений, связанных с политикой в области злоупотреблений DNS, до конференции в Панаме.Итак, на этом слайде вы можете увидеть все gTLD, у которых, по крайней мере, один зарегистрированный случай злоупотребления доменом за это время, и он показывает, знаете ли, разные цвета показывают, как эти сообщения о злоупотреблениях меняются со временем.Очевидно, что спам является лидером в плане отчетов, но мы видим фишинг, вредоносное ПО и ботнеты. В рамках системы DAAR или в OCTO одна из вещей, которые мы сделали, заключалась в следующем: мы взяли данные, созданные DAAR, и сделали такие пузырьковые диаграммы.Если бы у нас была анимация, вы бы увидели, что эти вещи растут и со временем

сокращаются. На самом деле, за этим интересно наблюдать, вы знаете, это как своего рода дисплей с гелевой лампой, если вам скучно. Это показывает злоупотребление доменами через фишинг, и в целом более крупные домены все находятся в пределах относительно узкой полосы.Следующий слайд. Вы начинаете видеть некоторых лжецов. То, что выходит из области так называемой статистической нормы. И мы намерены в будущем опубликовать имена, которые фактически дадут людям представление о том, какие из регистратур и регистраторов подвергаются большему количеству злоупотореблений, чем другие. Очевидно, что спам становится намного интереснее, и особенно когда вы меняете это со временем. Эти пузыри поднимаются, опускаются. Влево и вправо. Поэтому, на самом деле, это очень интересный дисплей, содержащий некоторую интересную информацию о так называемом переходе злоупотреблений из нескольких, из одной регистратуры в другую с течением времени.Следующий слайд. Таким образом, здесь показан процент разрешающих исторических доменов и новых gTLD. Как вы можете видеть, исторических по-прежнему,знаете ли, больше, чем новых gTLD, как с точки зрения спама или с точки зрения злоупотреблений, так и с точки зрения общего числа регистраций.Следующий слайд, пожалуйста. Процент злоупотреблений доменами. Процент злоупотребления доменами, указанными в DAAR. Опять же,

это показывает увеличение для исторических с течением времени и снижение среди новых gTLD.Одна из вещей, связанных с DAAR, - тем, кто заинтересован в злоупотреблениях, она предоставляет потрясающий объем данных, которые просто там сидят, а потом вдруг: что происходит? Это мою команду довольно хорошо развлекает, вероятно, к лучшему. Вы не хотите, чтобы эти люди выходили на улицу ночью! Следующий слайд. Где сосредоточены злоупотребления? Таким образом, эти статистические данные показывают, что существует относительно небольшое количество доменов, которые отвечают за подавляющее большинство злоупотреблений.Это то, что было известно, с чем вы вот уже некоторое время знакомы. DAAR предоставляет нам конкретные данные, которые на самом деле показывают это. Следующий слайд. Статус проекта. Следующий слайд. Как я уже говорил, наше внимание уделяется тому, чтобы все делать правильно, а не быстро. Как я уже упоминал, у нас есть отчеты рецензентов, мы настраиваем систему сбора данных, RBL, которую мы используем достаточно последовательно, чтобы обеспечить своевременное и надежное обновление.Версия 2 находится в стадии разработки. Мы надеемся автоматизировать большую часть отчетности, чтобы минимизировать объем ручного труда, чтобы обеспечить своевременное получение результатов.Мы изучаем гранулированную атрибуцию, и мы

экспериментируем с некоторыми дополнительными измерениями. Следующий слайд. Хорошо, это все. Одна из областей, которая нам представляется наиболее сложной в отношении DAAR в контексте сборе информации о регистраторах, является функцией WHOIS, ограничение допустимой частоты запросов, и в данный момент мы не уверены, у нас нет достаточной уверенности относительно данных о регистраторах, не уверены в необходимости их публикации в первом выпуске.Мы надеемся, что в более поздних версиях мы подумаем о том, как мы можем эффективно собирать данные регистраторов. И с этим, я думаю, я передам слово Фабьену, или если будут какие-то вопросы, я с удовольствием попытаюсь ответить на них.

CATHRIN BAUER BULST: Спасибо, Дэйв, за отличную презентацию, и я просто хочу сказать Вам, насколько мы благодарны ICANN за участие в этих усилиях. И я думаю, что это будет иметь решающее значение для усилий по разработке политики, поскольку это поставит под микроскоп то, какие проблемы заслуживают внимания в нашей разработке политики и где, возможно, необходимо изменить или улучшить процедуры для борьбы с определенными типами системных злоупотреблений, которые не ослабевают. Я подумала, что было бы интересно услышать, что должно произойти, как вы думаете, до того, как

эта инициатива будет в состоянии фактически публиковать информацию о том, где злоупотребления имют место относительно конкретных доменов, регистратур. Регистраторов и т.д.?

DAVID CONRAD: Как я уже упоминал, основное внимание, которое мы уделяем до публикации имен, связанных с данными, которые мы видим, - это получить независимый сторонний обзор, чтобы убедиться, что вы, что мы не делаем ничего глупого или недалекого с данными, чтобы свести к минимуму вероятность появления ложных сообщений о том, что люди неправильно признаны как источник злоупотреблений DNS, и попытаться обеспечить уровень доверия к сообществу, чтобы данные, которые мы предоставляем, были пригодны для вас, конкретная информация, ориентированная на данные, для разработки политики.Как я уже упоминала, один из независимых рецензентов уже завершил свою работу. Второй должен будет закончить, надеюсь, через нескольких недель, а затем, как только это будет сделано, мы сделаем эти отчеты доступными, а затем начнем процесс генерации отчетов для публикации сообществу, указывающих, вы знаете, какова статистика на самом деле и кто является участником в рамках этой статистики.

CATHRIN BAUER BULST: И Вы упомянули термин "превышение допустимой частоты запросов", и я не уверена, что все поняли, что это значит, и я надеялся, что Вы дадите нам краткое объяснение.

DAVID CONRAD: Конечно.Таким образом, любая услуга сети может подвергаться атаке типа «отказ в обслуживании» или атаке, которая инициирует соединение быстрее, чем возможности системы, поэтому довольно распространенная практика для операторов сети и операторов услуг заключается в наложении ограничений для сокращения количества подключений, которые могут произойти, в первую очередь для предотвращения злоупотреблений. В контексте регистратур и регистраторов ряд, по сути, насколько я знаю, все регистратуры и регистраторы налагали ограничение по допустимой частоте запросов, чтобы попытаться уменьшить количество людей, так сказать, копающихся в базе данных для получения контактной информации, которая будет использоваться для создания спама и другие векторов атаки. Таким образом, побочный эффект, однако, отражается на исследователях, которые пытаются собрать информацию для атрибуции регистраторам, имен доменов для регистраторов, это означает, что мы должны иметь дело с этими лимитами допустимой частоты запросов, и, вы знаете, в некоторых случаях эти ограничения допустимой частоты

запросов довольно экстремальные, например, можно отправить только 5 запросов в час или что-то в этом роде.Обоснование для ограничения допустимой частоты запросов, вы знаете, вполне разумно, и, вы знаете, это разумный механизм сетевых операций, и было бы неплохо, если бы мы могли понять, каким образом аккредитованные или признанные исследователи могут быть разблокированы, чтобы делать неограниченное количество запросов, но мы все еще пытаемся решить этот вопрос в данный момент.

CATHRIN BAUER BULST: Большое спасибо Дэйву, и это Катрин для стенограммы. И просто подчеркну суть ответственности отдельных участников. Я понимаю, что была одна конкретная жалоба на конкретного регистратора, который, используя ваши дипломатические термины, страдает от или подвергается непропорционально большому количеству злоупотреблений, и я понимаю, что одна из проблем, связанных с жалобой, заключается в том, что она основана на отчете SADAG, который основан на данных января 2017 года.Так что он не опирается на самые свежие данные , и я думаю , что в этой связи докладе DAAR будет иметь значение , поскольку он поддерживает постоянный и непрерывный анализ злоупотреблений по мере их развития в отношении конкретных субъектов и будет содействовать такого роду

прозрачности, которая, в конце концов, также, надеюсь, будет продвигать усилия по соблюдению, поэтому мы очень ценим работу, которую вы делаете, и у нас заканчивается время, но я просто хочу узнать, хочет ли кто-нибудь задать какие-либо заключительные вопросы, прежде чем мы закроем эту сессию?

LAUREEN KAPIN: У меня есть последний вопрос, который, я думаю, будет хорошим следствием наших обсуждений, и, конечно же, вы знаете о возможных изменениях в системе WHOIS, и мне интересно, как, на Ваш взгляд, это может повлиять на инициативу DAAR.

DAVID CONRAD: К счастью, система DAAR не использует персональную идентификационную информацию.Единственная информация, которую DAAR использует в ICANN, по крайней мере, в связи с созданием отчетов, о которых мы говорим, - это информация о регистраторах, связанная с доменным именем.Вся другая информация полезна, когда вы фактически пытаетесь разобраться и пытаетесь понять, знаете ли, какого-либо конкретного вектора атаки или что-то в этом роде, но для целей создания отчета информация о регистраторе является единственной информацией, которая нам

действительно нужна. В теории. По крайней мере, эта информация должна быть доступна через общественную WHOIS, вы знаете, без ограниченного доступа, но вы знаете, и все знают, что ведутся обсуждения в настоящее время, и окончательное решение о том, какая, знаете ли, какая информация будет общедоступной, по-прежнему, как я знаю, все еще не принято.

LAUREEN KAPIN: Так что это ... усилия инициативы. Это принесет пользу сообществу, и я также знаю, что это большая работа, поэтому мы ценим это. Таким образом, можно закрыть первую часть этой дискуссии по PSWG, которая включала наш Рабочий план, а затем обсуждение конкретной инициативы ICANN, которая поможет пролить свет на то, где происходят злоупотребления DNS, и информировать сообщество о тенденциях, поэтому это может стимулировать разработку политики. Итак, мы закрываем эту тему, а вуаля - сейчас мы переходим ко второй теме.А именно WHOIS и GDPR. Поэтому я передам слово руководству GAC.

[КОНЕЦ СТЕНОГРАММЫ]