ICANN71 | Виртуальный форум по формированию политики – пленарное заседание: Основные сведения о списках блокировки ресурсов с плохой репутацией
Четверг, 17 июня 2021 года, 10:30 – 12:00 по CEST

БРЕНДА БРЮЭР: Начинаем наше заседание. Включите запись.

**[Идет запись.]**

БРЕНДА БРЮЭР: Здравствуйте! И добро пожаловать на пленарное заседание ICANN71 «Основные сведения о списках блокировки ресурсов с плохой репутацией».

Меня зовут Бренда Брюэр (Brenda Brewer), и на этом заседании я исполняю обязанности координатора удаленного участия. Обратите внимание, что заседание записывается, и мы соблюдаем Стандарты ожидаемого поведения ICANN.

Во время заседания будут зачитываться только те вопросы и комментарии, которые отправлены с помощью функции вебинара Q&A. Я буду зачитывать их в указанное председателем или модератором этого заседания время. На этом заседании будет выполняться устный перевод на

английский, китайский, французский русский, испанский и арабский языки. Нажмите кнопку перевода в Zoom и выберите язык, на котором вы хотите слушать это заседание. Если вы хотите высказаться, поднимите руку в Zoom. И после того как координатор заседания назовет ваше имя, наша команда технической поддержки даст вам возможность включить микрофон.

Прежде чем говорить, убедитесь, что вы выбрали язык, на котором будете говорить, в меню перевода. Назовите для протокола свое имя и язык выступления, если это не английский.

Когда будете говорить, отключите звук и уведомления на всех остальных устройствах. Пожалуйста, говорите четко и с нормальной скоростью, чтобы обеспечить точный перевод.

Все участники заседания могут оставлять в чате комментарии. Для этого выберите пункт «Ответить всем участникам группы и присутствующим» в раскрывающемся меню чата. После этого все смогут увидеть ваш комментарий. Обратите также внимание, что закрытые чаты в формате вебинара Zoom возможны только между участниками группы. Любое сообщение, отправленное участником группы или обычным присутствующим другому

обычному присутствующему, увидят организатор заседания, соорганизаторы и остальные участники группы.

Чтобы вывести на экран стенограмму в режиме реального времени, нажмите кнопку субтитров по требованию на панели инструментов Zoom. Ну а теперь я передаю слово Эл Джи Форсбергу (LG Forsberg). Спасибо.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Бренда. Меня зовут Эл Джи Форсберг, и я модератор этого пленарного заседания ICANN71, которое называется: «Основные сведения о списках блокировки ресурсов с плохой репутацией».

Для тех из вас, кто меня не знает, я ветеран доменной отрасли Швеции с опытом работы как у регистратора в качестве технического менеджера продукта и представителя по связям с регистратурами, так и в регистратуре на различных технических и связанных с каналами сбыта должностях.

В настоящее время я работаю CTO в компании iQ. Это коммерческий поставщик услуг для доменной отрасли, таких как iQ Abuse Manager и доменная аналитика.

Когда я не занимаюсь интеграцией очередного списка блокировки ресурсов с плохой репутацией в Abuse Manager, то также консультирую различные регистратуры и регистраторов по техническим вопросам и по вопросам политики.

И последнее, но не менее важное: я являюсь основателем и куратором Nordic Domain Days, ежегодной конференции скандинавских участников доменной отрасли, и жду не дождусь, когда же снова появится возможность личных встреч.

На сегодняшнем заседании мы обратимся к массам. Мы подготовили анкету с тремя вопросами, на которые вам предлагается ответить, слушая обсуждение. Два из них будут представлены сейчас. А последний появится перед заключительным разделом сегодняшней повестки дня.

Не могли бы вы вывести на экран вопросы анкеты.

БРЕНДА БРЮЭР: Спасибо. На экране вы видите первый вопрос. Знакомы ли вы со следующими видами угроз безопасности? Выберите все подходящие варианты ответа.

Предлагаются следующие варианты: «Спам», «Фишинг», «Вредоносное ПО», «Фарминг», «Ботнеты» и «Другие». Еще раз. Знакомы ли вы со следующими видами угроз безопасности? Выберите все подходящие варианты ответа: «Спам», «Фишинг», «Вредоносное ПО», «Фарминг», «Ботнеты», «Другие». Опрос завершится примерно через пять секунд.

Спасибо.

Давайте закончим с этим вопросом.

Можно вывести на экран вопрос номер 2?

Вопрос номер 2: Подвергалось ли доменное имя, находящееся под вашим управлением, одной из этих угроз безопасности? И можно ответить «Да», «Нет» или «Не знаю»... или «Я не управляю доменами». Извините, здесь четыре варианта. Выберите один. Еще раз. Подвергалось ли доменное имя, находящееся под вашим управлением, одной из этих угроз безопасности? «Да», «Нет», «Не знаю» или «Я не управляю доменами».

И у вас есть еще пять секунд для ответа.

Большое спасибо.

Можно завершить опрос.

Эл Джи, возвращаю микрофон вам.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Бренда.

Я продолжу кратким введением в тему, прежде чем мы перейдем к разделу тематических дискуссий. Среди сегодняшних слушателей есть ряд сторон, которым необходимо использовать списки блокировки ресурсов с плохой репутацией по-разному. К этом сторонам, я бы сказал, относится ICANN, которая предоставляет статистику в DAAR, используя списки блокировки ресурсов с плохой репутацией, а также требует, чтобы новые gTLD контролировали хотя бы свои (неразборчиво).

Есть связанные договорными обязательствами стороны, регистратуры и регистраторы, которые могут использовать один или несколько списков блокировки ресурсов с плохой репутацией для мониторинга своих TLD или списка зарегистрированных доменных имен в случае регистраторов.

Есть поставщики услуг, например хостинговые компании, которые могут использовать списки блокировки ресурсов с

плохой репутацией, чтобы защитить электронную почту своих клиентов от спама или убедиться, что не поступали сообщения о применении размещенных у них сайтов для неблаговидных вещей, таких как фишинг или распространение вредоносного ПО.

Наконец, есть конечные пользователи, которые в рамках этого обсуждения определяются как владельцы доменов или операторы доменных имен и сайтов. Сегодня они, по-моему, являются единственной из присутствующих здесь групп, возможно, не желающей иметь никакого отношения к спискам блокировки ресурсов с плохой репутацией.

То сеть списки блокировки ресурсов с плохой репутацией, разумеется, будут означать разные вещи в зависимости от того, к какой из этих групп вы себя относите. Для ICANN, регистратур или регистраторов это, скорее всего, будет инструментом, который используется вами или вашим партнером, в то время как для конечного пользователя это может означать катастрофу, если в конечном итоге отправленное вами письмо попадет в черную дыру — папку нежелательной почты — или вместо вашего сайта в Chrome будет отображаться красный экран смерти Google.

Кроме того, название темы могло сказать вам о том, что сегодня мы не собираемся проводить 90-минутное обсуждение определение понятия «злоупотребление DNS», хотя списки блокировки ресурсов с плохой репутацией являются неотъемлемой составляющей обсуждения злоупотреблений DNS. Вместо этого мы собрались здесь, чтобы получить немного больше информации о том, как работают списки блокировки ресурсов с плохой репутацией, и о том, каким образом мы, аудитория, — связанные договорными обязательствами стороны, поставщики услуг и конечные пользователи — можем с ними работать.

Сегодня мы многое услышим о списках блокировки ресурсов с плохой репутацией, но еще одно упрощенное предварительное описание не повредит.

Итак, список блокировки ресурсов с плохой репутацией — это набор указаний или отчетов, предлагаемых для предотвращения неправомерного поведения тем или иным образом. Слово «репутация» в названии часто означает наличие некоторых оттенков серого в их способе определения, следует ли включать доменное имя в список или нет. Часто это не просто «да» или «нет».

Примером является реализация репутации компанией Spamhaus, где каждое доменное начинает с нуля и набирает отрицательные баллы за хорошие действия и положительные за плохие.

Как только будет набрано достаточное количество баллов, например пять или десять, доменное имя вносится в список блокировки.

Слово «блокировка» в названии отдает дань уважения причине появления этих провайдеров, поскольку эти списки были внедрены или внедряются на почтовых серверах и брандмауэрах для предотвращения спама или нежелательного трафика. Эти списки использовались и используются для блокировки.

Так что борьба со злоупотреблениями... извините. Конечно.

Так что борьба со злоупотреблениями может быть не единственным примером использования, а иногда даже не основным примером использования.

Некоторые списки блокировки ресурсов с плохой репутацией предложат полный перечень информации о том, как был обнаружен определенный плохой ресурс, тогда как другие

просто намекнут вам, что с определенным доменным именем произошло что-то плохое.

Кажется, у большинства списков репутации есть кое-что общее: не всегда легко понять, что они делают, как они это делают и чем могут помочь их данные, особенно если вы конечный пользователь, не имевший ранее никакого отношения к этим видам ресурсов.

Но чтобы попытаться разобраться в том, как поставщики списков блокировки ресурсов с плохой репутацией собирают данные и систематизируют свою информацию, а также чтобы по настоящему глубоко вникнуть в то, каким образом эта машина в некотором смысле перемалывает данные, периодически выдавая новый список, мы собрали здесь сегодня несколько представителей поставщиков списков блокировки ресурсов с плохой репутацией, и к нам также присоединилась группа представителей сторон, перечисленных ранее, чтобы рассказать о своем опыте работы со списками блокировки ресурсов с плохой репутацией.

С этими словами я хотел бы познакомить вас с первым участником и предоставить ему возможность представить себя и компанию, где он работает.

Пожалуйста, господин Карел Биттер (Carel Bitter) из Spamhaus.

КАРЕЛ БИТТЕР: Доброго дня всем! Меня зовут Карел Биттер. Я работаю в Spamhaus, где в основном занимаюсь вопросами репутации доменов. Мы создаем несколько массивов данных, но сегодня давайте сосредоточимся на той части нашей деятельности, которая относится к доменам.

Я занимаюсь вопросами репутации доменов уже более десяти лет. И да, я уже участвовал в целом ряде заседаний и других мероприятий ICANN.

Мы рады помочь и ответить на все вопросы, которые могут возникнуть.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Карел.

Господин Роман Хьюсси (Roman Huessy) из abuse.ch, представьтесь, пожалуйста.

РОМАН ХЬЮССИ: Да, я Роман Хьюсси — основатель abuse.ch. Abuse.ch — это некоммерческий проект, который реализуется Бернским университетом прикладных наук. Его целью является сбор данных о ботнетах и не только, а также бесплатная и открытая публикация соответствующей информации.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Роман.

И наш последний участник, представляющий сегодня поставщиков списков блокировки ресурсов с плохой репутацией, господин Бен Кун (Ben Coon) из WMC Global.

Представьтесь, пожалуйста.

БЕН КУН: Спасибо. Бен Кун, WMC Global. Мы, главным образом, управляем антифишинговой платформой. Мы предоставляем списки блокировки фишинговых URL-адресов поставщикам SMS и брандмауэров, а также людям, которые в первую очередь становятся жертвами фишинга, цель которого — получение учетных данных через множество приманок.

Буду рад ответить на все вопросы. Спасибо.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Бен.

Что касается других сторон, участвующих в обсуждении, вначале я хотел бы представить Саманех Таджализадехуб (Samaneh Tajalizadehkhoob) из ICANN. Представьтесь, пожалуйста. И если есть какие-то основные моменты, которые вы хотели бы обсудить во время этой дискуссии, то сейчас самое время о них сказать.

САМАНЕХ ТАДЖАЛИЗАДЕХУБ: Всем привет. Меня зовут Саманех Таджализадехуб. Я работаю в офисе CTO ICANN в группе по вопросам безопасности, стабильности и отказоустойчивости. Я также руковожу проектом DAAR и имею предыдущий опыт работы в секторе науки и образования с каналами данных о репутации.

Поэтому сегодня я буду больше говорить о том, как и в каких проектах корпорация ICANN просматривает и использует эти каналы.

Спасибо.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Саманех.

Теперь я хотел бы представить господина Мэтта Томаса (Matt Thomas) из Verisign. Пожалуйста, представьтесь и расскажите о том, какие основные моменты вы хотите обсудить.

МЭТТ ТОМАС: Спасибо. Меня зовут Мэтт Томас. Я работаю в Verisign заслуженным инженером в отделе стратегии и исследований кибербезопасности.

Кроме того, я являюсь членом SSAC ICANN и в настоящее время занимаю должность заместителя председателя совета директоров M3AAWG. На сегодняшнем заседании мне хотелось бы обсудить различные варианты использования RBL.

Спасибо.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Мэтью.

Со стороны регистраторов сегодня к нам присоединилась Редж Леви (Reg Levy) из Tucows. Пожалуйста, представьтесь и расскажите о том, какие основные моменты вы хотите обсудить.

РЕДЖ ЛЕВИ: Здравствуйте. Меня зовут Редж Леви, я возглавляю в Tucows отдел контроля за соблюдением требований. Я также вхожу в состав группы по борьбе со злоупотреблением DNS, представляя там группу заинтересованных сторон-регистраторов. Фактически я сопредседатель рабочей группы по борьбе со злоупотреблением DNS.

Доброе утро. По видимому, я еще не до конца проснулась.

С нетерпением жду этого обсуждения.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Редж.

И последняя по очереди, но не по значимости, Джоанна Кулеша (Joanna Kulesza) из сообщества At-Large. Пожалуйста, представьтесь и расскажите о том, какие основные моменты вы хотите обсудить.

ДЖОАННА КУЛЕША: Спасибо Эл Джи. Спасибо, что пригласили нас. Спасибо, что пригласили меня и дали мне возможность выступить от имени конечных пользователей.

Я сопредседатель Консультативного комитета At-Large. Я занимаюсь вопросами наращивания потенциала и действительно считаю, что в этом обсуждении, в этом заседании экспертной группы и в списках блокировки ресурсов с плохой репутацией есть такая составляющая как наращивание потенциала.

В качестве основного момента, и это просто опровержение, судя по самому опросу и участию сообщества At-Large, неправильно считать, будто конечные пользователи не заинтересованы в списках блокировки ресурсов с плохой репутацией. Как раз наоборот. И я постараюсь донести эту мысль в процессе дальнейшего обсуждения.

Я рада находиться здесь. Спасибо, что пригласили меня.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Джоанна.

Теперь мы перейдем от вводного раздела этого заседания к первому разделу бесед на тему списков блокировки ресурсов с плохой репутацией и постараемся расширить наши знания о том, как они работают.

Я хотел бы начать этот раздел, попросив Карела дать определение списку блокировки, как он его понимает.

КАРЕЛ БИТТЕР: Это хороший вопрос. Начнем с блокирующей части.

Думаю, что во многих случаях это не просто полезная блокировка. И если рассматривать работу регистратур и регистраторов в целом, когда регистратуры или регистраторы просматривают данные для поиска проблемных доменов или проблемных клиентов, они на самом деле не занимаются блокировкой как таковой. Это скорее пример использования для исправления ситуации.

Поэтому лично я обычно говорю о наших массивах данных, а не о наших RBL, особенно в таком контексте. И я считаю это очень важным аспектом, который нужно учитывать всякий раз, когда вы начинаете работать с любым массивом данных. Для чего он предназначен? И что вы с ним делаете? Используете ли вы его по назначению? Используете ли вы его так, как он был... для чего он был предназначен?

А если нет, и я хочу сказать, что вам следует... я не говорю, что вы не можете использовать то, что предназначено для одной цели, для другой. Но вы должны знать, что ваш пример

использования может немного отличаться от использования другой стороной.

Как вы уже упомянули, наши системы работают следующим образом: мы фактически начисляем баллы доменам. При этом, чем выше оценка домена, тем больше у нас уверенности в том, что действительно происходит что-то плохое. И это позволяет действовать по-разному в зависимости от градации оценки.

Так что я думаю, да, вам действительно требуется понимание данных, с которыми вы работаете. А если его нет, то нужно обратиться к людям, создающим эти данные, и сказать: «Послушайте, я на самом деле не понимаю эту часть» или «Я пытаюсь поступить вот так. Это умная мысль?». Возможно, вы захотите заблокировать что-то конкретное в контексте электронной почты, но может быть не в контексте уровня DNS. Хорошим примером могут служить сокращенные ссылки. Сокращенные ссылки в электронном письме — широко известный признак проблемного письма. Любая законная электронная почта обычно не содержит сокращенных ссылок.

Но блокировка сокращенных ссылок на уровне DNS, пожалуй, будет слишком суровой мерой по отношению к

вашим конечным пользователям. Так что здесь определенно следует учитывать многое.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Карел.

Я хотел бы задать два дополнительных вопроса, касающихся Spamhaus. Это следующие вопросы: Какие типичные виды доказательств Spamhaus сочтет достаточным основанием для внесения доменного имени в список блокировки ресурсов с плохой репутацией? И передаются ли эти доказательства каким-либо образом сторонникам использования ваших массивов данных?

КАРЕЛ БИТТЕР: В нашем случае не всегда легко поделиться доказательствами, потому что все данные, которые мы получаем, поступают от интернет-провайдеров и других сетей, заключивших с нами соглашение об обмене данными, но мы не всегда можем делиться ими. Если люди в чем-то сомневаются, мы всегда открыты для вопросов.

Что касается использования данных регистратурами и регистраторами, с которым мы сотрудничаем, существует канал поддержки, позволяющий людям сказать: «Эй, мы

видим это в списке, но на самом деле не понимаем, что здесь происходит». Может, это ложноположительный результат? Что-то еще происходит? Мы всегда можем взглянуть на это и, возможно, поделиться дополнительными сведениями. Но они не... они не распространяются по умолчанию. Например, если вы получаете список, скажем, 100 плохих доменов, он не содержит также 100 образцов спама или 100 двоичных файлов вредоносного ПО. По сути, нам приходится в индивидуальном порядке определять, какой информацией мы можем поделиться, а какой нет.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Карел.

Роман, что касается этой темы, чем отличается подход abuse.ch?

РОМАН ХЬЮССИ: Извините. Не могли бы вы повторить первоначальный вопрос? Я как раз отвечал на вопросы в модуле вопросов и ответов.

ЭЛ ДЖИ ФОРСБЕРГ: Прошу прощения. Это не проблема. Итак, какие типичные виды доказательств злоупотреблений abuse.ch сочтет

достаточным основанием для внесения доменного имен в свой массив данных?

РОМАН ХЬЮССИ: Это хороший вопрос. Спасибо.

Итак, обычно доказательством считается обнаружение вредоносного ПО на взломанных сайтах или регистрация доменных имен злоумышленником.

Это означает, что система проверяет фактически каждую отправку на предмет наличия дополнительной вредоносной нагрузки. И в таком случае доказательства фактически публикуются на сайтах проекта, чтобы каждый мог их использовать. Кроме того, сообщение о злоупотреблении отправляется соответствующей хостинговой компании.

То есть проект довольно прозрачен с точки зрения предоставления доказательств, поскольку все доказательства публикуются на сайте и каждый может проверить, почему ресурс включен в список.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Роман.

Для понимания массива данных, можете ли вы описать жизненный цикл типового сообщения о вредоносном ПО, с первого... с момента, когда оно впервые было вам отправлено, до исчезновения угрозы?

РОМАН ХЬЮССИ: Разумеется. Что касается вредоносного ПО, это более или менее простая тема, в отличие от доменов для фишинга или спама, поскольку я жду определенного ответа от удаленного хоста. Это означает, что я могу без труда автоматически проверить, является ли сайт до сих пор источником вредоносного ПО. Я делаю это автоматически. И как только вредоносный контент исчезает, сайт или доменное имя автоматически помечаются как исключенные. Это фактически означает, что доменное имя или URL-адрес автоматически исчезают из списка блокировки, который я предоставляю.

Положительным аспектом такого подхода является то, что URL-адрес остается в списке только до тех пор, пока действительно создает угрозу. И проверка на сохранение угрозы выполняется несколько раз в час, обычно каждые десять минут.

Таким образом, сразу после устранения угрозы конечным пользователем домен или URL-адрес автоматически исчезают из списка блокировки, как правило, в течение часа.

С другой стороны, если проблема на самом деле не была устранена, скажем, вредоносный контент был просто удален без устранения основной причины, такой подход означает, что после повторной загрузки злоумышленником вредоносного контента система снова выполнит автоматизированную проверку. И если такой контент появится вновь, доменное имя или URL-адрес будет опять автоматически включено в список.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Роман.

Бен, можно ли сказать, что описанное Карелом и Романом значительно отличается от подхода WMC Global с точки зрения сообщений о фишинге, их жизненного цикла и доказательств фишинга?

БЕН КУН: Я бы сказал, что модель WMC Global в основном совпадает с моделью, о которой рассказал Роман.

Мы проверяем вредоносность сайтов, прежде чем включить их в список. Когда мы предоставляем список блокировки, скажем, провайдеру SMS для прекращения рассылки сообщений, обычно он использует только список за последние 24 часа, так как фишинговые сайты отключаются от интернета. Мы повторно вносим фишинговый сайт в список, если он появляется снова. Для анализа жизненного цикла, продолжительности существования этого фишингового URL-адреса, мы выполняем автоматические проверки.

Есть еще одно отличие того, что предлагаем мы, от того, что предлагается некоторыми другими списками блокировки. В наш список вносятся не домены, а полные URL-адреса. То есть вы можете точно увидеть, где находится вредоносный контент. И опять же, после отключения этого вредоносного контента от интернета он исключается из списка до тех пор, пока вновь не появится в сети.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Бен.

Карел, я снова обращаюсь к вам. Вы упомянули ранее, что пользователь списка блокировки ресурсов с плохой репутацией должен понимать, для чего предназначен этот список.

Какой пример использования в случае Spamhaus, по вашему мнению, является основным? То есть какого основного пользователя вы пытаетесь обслуживать? И считаете ли вы, что, скажем, за последние десять лет ситуация изменилась?

КАРЕЛ БИТТЕР: Безусловно, поскольку в названии нашей компании есть слово «спам», мы занимаемся электронной почтой.

Массив данных... эта работа немного сложнее. Массив данных, который мы открыто публикуем, список доменов для блокировки отражает наше представление о том, у каких доменов в настоящее время плохая репутация. В основном он используется для электронной почты, хотя там также есть домены с вредоносным ПО. Также в него включены серверы управления сетями зараженных машин. Там есть и фишинговые домены, все домены, которые мы считаем плохими, в одной большой куче.

Для разделения по категориям в данном случае используются коды возврата DNS. То есть можно выделить отдельную часть, например, только фишинг или только вредоносное ПО.

Наша задача — предоставить данные. Мы почти не контролируем их дальнейшее использование. Итак,

информация в формате публикации, общедоступная бесплатная версия, в основном используется на почтовых серверах. Так что это черный список DNS. Вы отправляете DNS-запрос, получаете ответ и обрабатываете его в соответствии со своей локальной политикой.

Есть несколько версий для конкретных угроз и примеров использования. При этом доступны различные выборки данных, например, для использования на уровне резолверов DNS. Существуют версии, предназначенные для расследования и устранения проблем регистратурами и регистраторами.

Итак, какой же пример использования является основным? Наверное, основной пример использования — это принятие людьми решений о репутации, исходя из доменного имени.

Я бы не сказал, что это нужно только для электронной почты. Возможно, так было в прошлом, но в наши дни, конечно, ситуация изменилась.

Большинство доменных имен, используемых для вредоносного ПО и ботнетов, как вам объяснит Роман, вы никогда не встретите в электронном письме. То есть вы можете проверять все свои электронные письма на предмет наличия этих

доменов, но просто никогда их не увидите. Они используются на другом уровне, когда зараженный компьютер обращается к определенному доменному имени, чтобы связаться с его центром ручного управления для загрузки дополнительного вредоносного ПО.

Это означает, что проверку упоминания этих доменных имен нужно выполнять не на вашем почтовом сервере, а на резолвере DNS, в IDS или другом аналогичном месте.

Таким образом, пример использования на самом деле зависит от того, какую именно проблему вы пытаетесь устранить.

Как сказал Бен, что касается проверки SMS, к примеру, множество доменов, которые встречаются в SMS или сокращенных ссылках, перенаправляющих на другой домен, вы никогда не увидите в электронном письме.

Так что это намного шире, по-моему, чем просто электронная почта. Если у вас есть проблема безопасности, к которой причастны доменные имена, то создаваемые нами, Романом или Беном массивы данных могут способствовать ее решению или пониманию происходящего.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Карел.

Теперь у меня вопрос ко всем троим поставщикам списков блокировки ресурсов с плохой репутацией. Мы слышали, как все вы немного рассказали о способах получения и сбора сообщений или показаний. И из этого видно, что мы говорим в основном о сообщениях или машинном обнаружении, о сканировании интернета и так далее или о просмотре электронных писем, к которым у вас есть доступ.

Проводились ли когда-либо при составлении списков блокировки в ваших компаниях расследования с привлечением людских ресурсов? Давайте начнем с Бена.

БЕН КУН: Да. У нас есть множество охотников за угрозами, которые перепроверяют или выборочно проверяют значительную часть обнаруженных случаев фишинга учетных данных. Мы также вручную анализируем все, что не набрало достаточно баллов для автоматического включения в наш список блокировки ресурсов с плохой репутацией, прежде чем добавить это в список.

Кроме того, персонал повторно рассматривает все виды ложноположительного срабатывания. Проводится расследование и ресурс добавляется либо удаляется вручную.

Но я бы сказал, что у нас довольно активное вмешательство человека.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Бен.

Роман.

РОМАН ХЬЮССИ: Да. Итак, что касается конкретно URLhaus, проекта, направленного на обнаружение сайтов с вредоносным ПО, то этот проект приводится в действие сообществом. Это означает, что создаваемые мной массивы данных — всего лишь одна часть. Другая часть создается сообществом.

И когда речь идет о сообществе, важно сказать, что есть два типа информаторов. Один тип — это, так сказать, посторонние информаторы. Это пользователи, которым я не доверяю. Вся поступившая от них в рамках проекта информация проверяется вручную.

С другой стороны, у нас есть надежные информаторы. И это означает, что при получении какой-то информации в рамках проекта от надежного информатора сайт автоматически будет включен в список. Однако система, конечно же, все равно проверит, имеется ли на сайте вредоносный контент. Но URL-адрес попадет прямо в базу данных.

Однако, если говорить об использовании в качестве списка блокировки, что является всего лишь одним из примеров использования этого массива данных, то, разумеется, сайт или доменное имя появится в списке только тогда, когда там действительно есть вредоносный контент.

И если ответить на ваш вопрос кратко, то это сочетание ручной и машинной проверки URL-адресов или доменных имен.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Роман.

Карел?

КАРЕЛ БИТТЕР: Да. В нашем случае это смесь автоматизации и расследований, выполняемых людьми. Если вы хотите оценить репутацию всех

существующих на планете доменных имен, то, очевидно, вам понадобится автоматизация. Их просто слишком много... вокруг слишком много доменных имен и ежедневно появляется слишком много новых доменных имен, чтобы люди могли все рассмотреть и изучить.

Так что автоматизация применяется, хотя в ней, бесспорно, присутствует человеческий фактор, то есть наши эксперты анализируют подозрительные данные, когда оценка достаточно близка к порогу невключения в список или когда вы говорите: хорошо, я ожидал, что будет набрано больше баллов, но это не так. Так что всегда имеет место сочетание человеческого и машинного интеллекта.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Роман.

Выделенное для этой части заседания время истекает. Однако есть популярный вопрос, который мне хотелось бы вынести на обсуждение. Насколько высока вероятность того, что вы признаете сообщение или показатель ложноположительным? И какова наиболее распространенная причина этого? Давайте начнем с Бена.

БЕН КУН: Я бы сказал, что среди данных в списках блокировки всегда есть ложноположительные. Мы стремимся максимально снизить количество таких ложных срабатываний.

Я бы сказал, что основная причина ложноположительных срабатываний — это непонимание того, что является вредоносным, а что нет, или когда люди получают то, что им просто не нравится, и сообщают об этом как о чем-то вредоносном, хотя это не так.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Бен.

Роман.

РОМАН ХЬЮССИ: Да, конечно, бывают ложноположительные срабатывания. Они всегда есть. И каждый может сообщить о них через пользовательский веб-интерфейс.

Если надежный информатор, например, начнет передавать данные, которые не являются известными вредоносными программами, скажем, фишинговыми или спам-сайтами или другими подобными вещами, то он будет просто заблокирован и исключен из проекта.

Так что поток данных, на мой взгляд, неплохой. Но как я уже сказал, ошибки возможны.

ЭЛ ДЖИ ФОРСБЕРГ: И наконец, Роман. Нет, последний Карел. Извините.

КАРЕЛ БИТТЕР: Да, ложноположительные срабатывания всегда происходят. И, как сказал Бен, наша задача — сделать так, чтобы их было как можно меньше.

Что касается сообщений от пользователей, вы знаете, много лет назад, когда провайдеры электронной почты начали включать кнопку «Это спам» в свои веб-интерфейсы, чаще всего люди использовали ее для сообщений о том, что на самом деле не было спамом или вредоносными письмами. Это были письма, которые им просто не нравились, например, счета, которые они не хотели оплачивать, или письма с отказом в приеме на работу. Так что в данном случае большинство систем работает следующим образом: если сообщения поступили от достаточного количества людей, если накопилась определенная критическая масса таких сообщений, то автоматизация срабатывает в отношении признаков плохой репутации IP-адреса, доменного имени, отправителя, сигнального селектора или чего-то еще.

И всегда есть вероятность, особенно если вы в своей работе учитываете информацию, поступающую от пользователей, что люди будут сообщать о вещах, которые, как сказал Бен, им просто не нравятся, то есть это не спам, не вредоносные программы и не фишинг. Но для многих нет разницы между кнопкой «Удалить» и кнопкой «Это спам».

Так что да, это всегда вызывает беспокойство. Но, разумеется, если задуматься, и это наверное также относится к Роману и Бену, ложноположительные данные в наших массивах и проблемы будут всегда. Может не происходить ничего плохого в течение недели, а на следующей неделе могут возникнуть три, четыре, пять ошибок, сколько угодно. Суровая реальность жизни в том, что они произойдут. Понимаете, важно то, как вы справляетесь с этим, насколько быстро удаляете их оттуда, обеспечиваете решение проблем должным образом.

Но, конечно, как поставщики и создатели данных, мы заинтересованы в том, чтобы наши данные были настолько хороши, насколько это возможно. Вы знаете, если наши данные будут плохими, то люди просто перестанут ими пользоваться, и тогда в чем смысл?

Что касается создателей данных, и я думаю, что в первую очередь Роман, возможно, с этим согласится, данные становятся тем мощнее, чем больше людей начинают их использовать. Если есть доменное имя, которое применяется, скажем, в системе управления и контроля ботнета, то чем быстрее это доменное имя будет удалено или чем больше людей заблокирует его, тем безопаснее станет интернет.

И если мы или Роман сообщим о нем, но при этом люди считают наши отчеты бесполезными, то это полностью противоречит нашей миссии.

Мы хотим, чтобы создаваемые нами данные использовались как можно шире, и мы хотим, чтобы люди с максимально возможным доверием относились к нашим отчетам, и чтобы интернет в конечном итоге стал более безопасным местом. Потому что, на мой взгляд, что касается всех троих, — меня, Бена и Романа, — именно это движет нашей работой. Мы пытаемся решить проблемы безопасности сетей, регистратур, регистраторов и, соответственно, конечных пользователей. В конце концов, все дело в защите конечного пользователя. И чем больше людей будет использовать данные, тем больше будет защищено конечных пользователей. И люди не станут использовать плохие данные.

Я имею в виду, что это очень важный аспект, которым мы всегда готовы заниматься.

Существует бесконечное множество способов действовать решительнее, когда вы говорите: ладно, если я сделаю это, то заблокирую больше, поймаю больше злоумышленников. Но есть много сценариев, когда где-то кто-то делает почти то же самое, что и злоумышленник, или использует такие же странные URL-адреса или имена хостов. Скажем, если я вижу такое имя хоста, то он обязательно должен оказаться плохим. Ладно, 99 из ста окажутся плохими, а вот последний — нет.

Так что это всегда вопрос баланса, и вам просто нужно постоянно стремиться к тому, чтобы работать максимально хорошо, насколько это возможно, и использовать подходящий процесс для решения всех возникающих проблем.

И я уже напечатал это, отвечая на один из вопросов, но у нас, например, любой может войти и удалить доменное имя. Вам не нужно... вам не придется заполнять длинные формы, связываться с нами по телефону или как-то еще. Это самообслуживание в интернете, как кнопка Романа.

Очевидно, что в наших интересах сделать процесс обработки любых ложноположительных данных как можно более

плавным для того, кто стал жертвой такого ложного срабатывания.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Роман. Позвольте вас прервать.

Идет та часть заседания, которая выделена для ответов на вопросы аудитории, и мне хотелось бы задать еще один вопрос, прежде чем мы перейдем к следующей части.

Я хотел бы спросить Романа, как... сотрудничают ли друг с другом поставщики списков блокировки ресурсов или данных об анализе угроз... назовем это исходными данными? К примеру, предоставляет ли abuse.ch, скажем, компании Spamhaus данные о ложноположительных срабатываниях или важные уведомления, которые могут у вас быть?

РОМАН ХЬЮССИ: Да, этот вопрос, который я считаю очень важным, уже поднимался в модуле вебинара Q&A.

Конечно, предусмотрены процессы передачи информации о текущих угрозах поставщикам или RBL. Некоторые из этих процессов двусторонние. Они есть, например, у Spamhaus, Safe Browsing и других поставщиков RBL. Но что касается

abuse.ch, этот массив данных доступен всем. Каждый может им воспользоваться. И значительная часть поставщиков информации о коммерческих угрозах использует эти каналы и делает с данными все, что хочет.

Поскольку регистрация не требуется, конечно, у меня есть проблема. Она заключается в том, что мне неизвестно, кто использует мой канал, являющийся открытым источником.

С другой стороны, что касается небольшого вопроса об обмене информацией о ложных срабатываниях, по-моему, это важная тема. И, насколько мне известно, в настоящее время нет механизмов, позволяющих сообщать об ошибочных включениях в список блокировки.

При обнаружении ложного срабатывания я, разумеется, решаю вопрос следующим образом: удаляю соответствующий ресурс из источника данных. И я рассчитываю, что остальные поставщики RBL или информации об угрозах также заметят у себя ошибку и удалят эту запись. Но, конечно, я никак не могу на это повлиять. По-моему, это было бы... эту тему нужно обсудить, чтобы создать платформу для обмена информацией, с помощью которой ложные срабатывания... сведения о ложных срабатываниях, например... можно было бы публиковать и передавать другим поставщикам.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Роман.

Мы подошли к той части заседания, которая выделена для презентаций ICANN. Поэтому я передаю микрофон Саманех.

САМАНЕХ ТАДЖАЛИЗАДЕХУБ: Всем привет. Для занесения в протокол: я Саманех Таджализадехуб (Samaneh Tajalizadehkhoob). Сегодня я представляю офис CTO ICANN и расскажу о списках блокировки ресурсов с плохой репутацией и нашем отношении к ним.

Спасибо. Следующий слайд, пожалуйста.

Итак, на данный момент уже состоялось хорошее обсуждение. По-моему, некоторые из затронутых в презентации моментов уже были охвачены другими участниками дискуссии, а также в ответах на вопросы. Извините за возможные повторения.

Я хотела начать с основы: что такое список блокировки ресурсов с плохой репутацией. Это может быть как список блокировки IP-адресов, так и список блокировки доменов. Как правило, все это объекты, которые считаются вредоносными, ненадежными или просто имеющими плохую репутацию. Я привела несколько примеров использования в

отрасли, исследованиях или в секторе науки и образования. И люди используют такой список как источник данных для брандмауэров DNS, чтобы предотвратить вредоносный трафик. Он также применяется для фильтрации нежелательного трафика, к которому обычно относится спам и фишинговые письма. Он используется сетями CDN для предотвращения доставки клиентам вредоносного контента, а также при реагировании на инциденты или в правоприменительной деятельности с целью выявления вредоносной инфраструктуры, участвующей в атаке.

У них разные механизмы распространения данных. Сегодня, по-моему, мы рассматриваем несколько примеров скорее открытых источников данных, но такие источники также могут быть коммерческими, доступными с ограничением скорости, на основе лицензии или с оплатой по факту использования, и могут быть... обычно поддерживаются коммерческими компаниями, специализирующимися на распространении информации об угрозах.

Существуют программы с открытым исходным кодом, которые используются в основном в научных кругах, но не только. Примерами являются Spamhaus, abuse.ch, PhishTank, с которым я знакома, и ряд других.

Они также могут специализироваться на определенных угрозах. То есть некоторые списки сосредоточены только на конкретных угрозах. Например, у ресурса abuse.ch, который поддерживает Роман, есть разные каналы данных, ориентированные либо на ботнеты, либо на вредоносное ПО, на программы-вымогатели, — по-моему, работа последнего сейчас прекращена, — и так далее, или носят общий, более общий характер. Они содержат данные обо всех видах угроз. Примером является SURBL.

Следующий слайд, пожалуйста.

Мы уже поговорили об этом и подробно обсудили. Заголовок этого слайда: «Особенности и недостатки списка». Я хочу уделить внимание обоим аспектам, поскольку то, что для одного исследователя является характеристикой, другой исследователь может счесть недостатком.

Итак, с нашей точки зрения, при использовании RBL важнее всего понять, что вы хотите сделать. И на самом деле еще важнее понять методику RBL, какие данные в нем представлены и как лучше всего использовать их для своих целей.

Особенности состоят в том, что некоторые списки могут быть узкоспециализированными, поскольку предназначены для определенной цели. Любой, кто хочет их использовать, должен понять эту цель и посмотреть, соответствует ли она его цели.

У некоторых... как правило... и вообще-то я говорю об этом как исследователь. Как правило, у некоторых списков ограниченный охват из-за физических ограничений и точек наблюдения. Обычно у поставщиков каналов данных конкретное географическое местоположение, поэтому они могут быть менее представлены в определенных географических точках.

Я знаю, что со временем, поскольку я работал над этим уже семь, восемь лет, со временем большинство списков улучшилось с точки зрения охвата, но все же важно всегда помнить об этом при анализе списков.

Есть один небольшой момент: идея изучения качества и различных показателей надежности списков блокировки не нова. Исследования ведутся с 2009, 2010 года. И в этой презентации я привожу неполный перечень проведенных научных и отраслевых исследований списков, но вы можете

связаться со мной для получения дополнительной информации, если она вам нужна.

Еще одна проблема или особенность RBL заключается в неполноте документации по внутренним методам. Одна из причин, как я поняла из бесед, личных бесед с поставщиками списков, заключается в том, что нелегко задокументировать все процессы, поскольку некоторые из них могут быть спонтанными, очень детализированными или могут меняться в ответ на возникшие обстоятельства. Поэтому сложно поддерживать в реальном времени документацию, где отражено все, что поставщик RBL делает с конкретным каналом данных.

Кроме того, поскольку у нас так много поставщиков RBL, они разные, как и следовало ожидать. Существует широкое разнообразие с точки зрения методологии, то есть с точки зрения сбора данных, курирования, поддержки и маркировки списков блокировки. Это по-разному влияет на охват, надежность, эффективность и скорость информирования.

Важно отметить, что это не обязательно плохо. На самом деле это могло бы приносить пользу. Разнообразие могло бы привести к росту объема доступной информации,

при условии что пользователь понимает разнообразие и правильно его использует.

Следующий слайд, пожалуйста.

Я уже сказала об этом. Итак, почему важно знать эти недостатки, иначе говоря, особенности? Прежде всего, каждому пользователю, будь то сетевые операторы, исследователи или охранные предприятия, опирающиеся на эти ресурсы, важно понимать различия между списками, их недостатки и нюансы для разработки более эффективных средств и методов защиты, а также помнить об этом при проведении исследования или подготовке отчетов о результатах.

Можно привести хороший пример, с которым я нередко сталкиваюсь в сообществе ICANN лично. Мы часто говорим: вот исследование, показывающее, что фишинг не прекращается... наблюдается тенденция роста объемов фишинга. Почему это противоречит результатам другого исследования, проведенного другим человеком, которое свидетельствует о тенденции их снижения?

Именно эту мысль я пытаюсь донести, и я думаю, что это основная мысль моего набора слайдов. В зависимости от

того, какой массив данных используется, в зависимости от того, какие временные рамки принимаются во внимание, какова процедура маркировки полученного набора данных и так далее, тенденция может меняться.

Так что ни один из каналов данных не позволяет однозначно определить тенденцию, по крайней мере, исходя из моего опыта, чтобы можно было с уверенностью утверждать, какая именно тенденция наблюдается. Данные всегда неполные, поэтому выводы всегда делаются с точки зрения конкретного канала. Роман, Карел и Бен уже несколько раз говорили: «это то, что мы видим с точки зрения нашего RBL». Так что данные всегда частичные и всегда зависят от методологии.

Следующий слайд, пожалуйста.

На нескольких следующих слайдах я выделю ряд примеров использования в ICANN. Итак, как мы используем RBL.

DAAR — платформа отчетности о случаях злоупотребления доменами — это один из основных проектов, где используется RBL. Возможно, большинство из вас с ним знакомо.

Не буду вдаваться в подробности работы DAAR, но в общих словах мы... система берет доменные имена из файлов зоны

регистратуры, а затем берет доменные имена из набора предварительно отобранных каналов данных о ресурсах, используемых для фишинга, распространения вредоносного ПО, управления ботнетами и рассылки спама как средства доставки вредоносного контента. Затем домены из файлов зоны сравниваются с доменами в RBL, выполняется обработка, вычисление ежедневных и ежемесячных показателей для различных видов анализа, с которыми вы, возможно, знакомы из ежемесячных отчетов ICANN... ежемесячных отчетов DAAR, которые публикуются на сайтах ICANN. Они показывают тенденции того, где концентрируются угрозы безопасности DNS в определенный момент времени и как эта концентрация меняется с течением времени.

При этом нужно иметь в виду, что система, разумеется, выполняет обширную предварительную обработку, очистку и унификацию используемых каналов данных RBL с учетом всех тупиковых ситуаций и так далее. Подробности изложены в методическом документе проекта.

Следующий слайд, пожалуйста.

БРЕНДА БРЮЭР: Извините. Прежде чем вы продолжите, я попрошу вас говорить медленнее для переводчиков. Спасибо.

САМАНЕХ ТАДЖАЛИЗАДЕХУБ: Разумеется.

Мы тоже реализовали один проект. Как исследовательская группа по SSR мы также реализовали один проект для поддержки отдела ICANN по контролю исполнения договорных обязательств и создали моментальные снимки показателей регистраторов. Так что это не... это был разовый проект, в рамках которого мы сделали то же самое, что и DAAR, но только для регистраторов. Основное внимание уделялось фишингу и вредоносному ПО за определенный период времени, всего лишь за несколько месяцев.

И мы рассчитали показатели для регистраторов и семейств регистраторов, показывающие концентрацию угроз в определенный момент и в динамике.

Для этого конкретного проекта нам был предоставлен доступ к BRDA, поскольку пока мы можем его использовать только в целях контроля за соблюдением обязательств.

Следующий слайд, пожалуйста.

Что касается других текущих исследовательских проектов OCTO, мы используем списки RBL для разработки моделей прогнозирования, чтобы иметь возможность предсказать, когда домен станет вредоносным, а также для извлечения шаблонов, характеризующих вредоносные домены.

Мы также собираемся воспользоваться методом, который аналогичен методу исследования COMAR, представленного во время Tech Day на предыдущей конференции ICANN, чтобы различать злонамеренно зарегистрированные и взломанные домены, используя RBL в качестве одного из источников входных данных.

Следующий слайд, пожалуйста.

Итак, как в настоящее время мы... или для большинства перечисленных на предыдущих слайдах проектов мы оценивали... или проводили оценку для выбора списка ресурсов с плохой репутацией, а также мониторинг каналов в течение определенного периода времени, прежде чем приступить к их использованию для нашей исследовательской работы.

По существу, мы на основе публикаций отобрали списки, наиболее авторитетные в секторе науки и образования и

отрасли. Оценка авторитета на основании публикаций может быть субъективной. И мы выбрали те, у которых лучше документация и стандартизация данных, лучше описаны процессы и они дополняют наши собственные стандарты с точки зрения охвата.

Да.

Следующий слайд, пожалуйста.

Однако мы планируем перейти к более строгим критериям оценки. Работа над этим идет.

И, опять же, мне хотелось бы подчеркнуть, что работа по оценке RBL уже выполнялась. Мы занимаемся этим только для повышения полноты и актуальности информации о современном состоянии каналов данных.

Итак, мы занимаемся разработкой показателей для того, что называем чистотой, то есть для количества ложноположительных и ложноотрицательных результатов в списке. Замечу в скобках, что эти показатели сложно оценить, учитывая сложность получения достоверных данных, то есть размеченных в этом массиве вручную; это на

самом деле первая проблема для любого исследователя, работающего с RBL.

Мы оцениваем охват списков, скорость отклика или получения ответа, достоверность и степень детализации данных в этом канале, стабильность с течением времени, а также актуальность данных — сколько доменов правомерно включено в список и активно на момент их появления в канале.

Перечень каналов еще не сформирован окончательно. Мы пытаемся работать над ними, чтобы понять, можно ли добиться надежных результатов. Они могут измениться со временем, пока мы работаем над исследовательским проектом, или остаться прежними. Но мы будем держать вас в курсе этой работы. Пока это просто незавершенная работа.

Следующий слайд, пожалуйста.

Вот источники, на которые я ссылалась во время презентации. И моя презентация подошла к концу.

Мне хотелось бы отметить еще один момент, поскольку мы как офис CTO ICANN ведем методом проб и ошибок несколько проектов с использованием RBL специально для регистратур

и регистраторов, чтобы попытаться предоставить больше информации об угрозах безопасности.

Ряд причин усложняет разработку определенных показателей, о которых сообщество говорило ранее, и мы не хотим публиковать что-то ненадежное. Именно этот вопрос мы обсуждаем в настоящее время.

Например, мы ранее говорили о времени безотказной работы, то есть о времени, которое требуется операторам для реагирования на определенные нарушения безопасности. Если вернуться к обсуждению, которое ведет группа участников, а также к материалам этой презентации относительно различий в методологии каждого списка, то можно быстро понять, что если взять несколько списков и попытаться создать показатель времени безотказной работы для конкретного оператора, мы смешаем разные методологии. И сам по себе такой показатель не предоставит заслуживающей доверия информации о каждом операторе. Кроме того, он зависит от методологии поставщика RBL.

И это примеры конкретных трудностей в наших проектах, с которыми мы пытаемся справиться.Но на самом деле полезно поднять этот вопрос для обсуждения в сообществе, и это была хорошая возможность.

Всем спасибо. Если у вас есть вопросы, буду рада ответить. Я не знаю, что у нас со временем.

ЭЛ ДЖИ ФОРСБЕРГ: Говорит Эл Джи Форсберг, модератор. Из-за нехватки времени мы перейдем к следующему разделу этого заседания.

И это будет заключительная часть обсуждения, во время которой я хотел бы обратиться к представителям сторон, связанных договорными обязательствами, присутствующим среди участников дискуссии, то есть к Реджу и Мэтью.

Я хотел бы спросить вас обоих, используете ли вы в настоящее время списки блокировки ресурсов с плохой репутацией, и если да, то как. Пусть сначала выскажется Редж.

РЕДЖ ЛЕВИ: Спасибо, Эл Джи.

В настоящее время Tucows не платит розничным поставщикам списков блокировки за их данные. Однако мы регулярно получаем сообщения от многих авторитетных лиц.

К сожалению, в большинстве сообщений, обычно отсутствует полный URL-адрес, поэтому нам трудно в каждом случае

смягчить последствия, так как не всегда удается точно определить, в чем именно состоит проблема в том смысле, имеем ли мы дело со взломанным доменом или недобросовестным владельцем домена?

Иногда мы можем это сделать. Мы можем взять этот домен, посмотреть на него в нашей системе и сказать: «Хорошо, да, он был куплен с мошенническим использованием кредитной карты». В таких случаях часто домен уже отключен еще до получения сообщения. Но мы все равно получаем сообщение о нем.

Так что в настоящее время мы не используем эти списки. В настоящее время мы рассматриваем некоторые из доступных вариантов. Для нас важна скорость исключения из списка блокировки. То есть мне недостаточно просто сообщить, что домен вредоносный, поскольку я также скажу: «Отлично, большое спасибо за сообщение, мы справились с этой проблемой», а затем попрошу удалить его из списка.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Редж.

Мэтью?

МЭТТ ТОМАС: Да. Мне хотелось бы указать еще на несколько моментов, касающихся полезности RBL, которые уже были отмечены некоторыми участниками дискуссии, и это скорее касается концепции контекста, которую начал поднимать Карел и упоминали другие участники.

Я считаю, что очень важно понимать контекст применения RBL. Прежде всего, следует сказать, что они являются весьма эффективными инструментами, если их использовать в надлежащем контексте. И я думаю, что это во многом связано с пониманием происхождения, изначальной цели создания этих RBL. Они разрабатывались как инструменты защиты конечных пользователей, сетей и сред.

Для такого примера использования они обладают определенными свойствами, соответствующими данной цели. Они могут быть чуть более либеральными с точки зрения... извините... того, что включают в RBL. Но они также могут быть чуть более консервативными с точки зрения удаления некоторых из этих записей.

И в контексте использования для корпоративной безопасности специалистом по безопасности это хорошее свойство, верно? В таком сценарии вас меньше волнуют

ложноположительные срабатывания, и больше беспокоит защита конечных пользователей.

Но когда вы начинаете использовать RBL в других контекстах, важно понимать свойства этих RBL и то, как эти свойства будут влиять на различные способы использования RBL для разнообразных измерений, инструментов или исследований. Знание нюансов создания, обслуживания, управления и проверки RBL в конечном итоге повлияет на вашу способность систематически использовать этот RBL любым другим образом.

Поэтому я считаю, что всем нам важно знать, как они используются, и применять их надлежащим образом.

Спасибо.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо.

РЕДЖ ЛЕВИ: Я хочу кратко подчеркнуть, что транспарентность в понимании того, как составляются RBL, чрезвычайно полезна для тех, кто использует свои данные.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Редж.

Опять же, Редж и Мэтт, можете ли вы сказать, что связанные договорными обязательствами стороны, регистратуры и регистраторы, могли бы сделать больше с помощью списков блокировки ресурсов с плохой репутацией, если какая-либо конкретная часть данных передавалась вам или обновлялась другим способом?

МЭТТ ТОМАС: Для занесения в протокол: говорит Мэтт Томас.

Это очень интересный вопрос, Эл Джи. И я думаю, что меня в этом вопросе поражает слово «больше». Что это значит? И как вы измеряете это «больше»?

Означает ли «больше» в контексте злоупотребления доменными именами, что будет отключаться больше доменов? Или это означает нашу более высокую эффективность разрушения и уничтожения базового инструментария инфраструктуры, поддерживающей распространенные виды злоупотребления DNS.

Так что, по-моему, нам следует взглянуть на общую картину, ведь в этой экосистеме есть не только RBL и стороны,

связанные договорными обязательствами. Все сообщество должно сосредоточить внимание на злоупотреблении DNS. Есть множество разных организаций, которым необходимо будет сообща поработать, чтобы сделать это более достижимым, верно?

Нам необходимо привлечь хостинг-провайдеров, CDN, почтовых провайдеров, правоохранительные органы. И, работая сообща, мы сможем начать борьбу со злоупотреблениями и сделать больше с использованием такого подхода.

Не сомневаюсь, что поставщики RBL могут привести массу примеров, когда они собирали данные, находили фишинговый домен, включали его в RBL, после чего он отключался от интернета, а через два часа или через день вместо него появлялась пара новых доменов. Разве такой подход к искоренению злоупотреблений принес больше пользы? Или он просто вызвал рассеивание имен и подтолкнул к совершению злоупотреблений с помощью этого домена в другом месте, так? Прекращается ли само злоупотребление?

То есть основная проблема в том, что нам нужно заниматься инфраструктурой и системными вещами, которые ее поддерживают.

Еще одним прекрасным примером, пожалуй, являются DGA и ботнеты. Я хочу сказать, взгляните, например, на Conficker, так? Ему уже десять лет, и он до сих пор существует, или Avalanche. По-прежнему приходится прилагать усилия для борьбы с этими видами злоупотребления DNS, так как основная реальная проблема заключается в отсутствии исправлений на хост-узлах и в базовых системах, верно?

И поэтому можно ответить на последнюю часть вашего вопроса, Эл Джи, о том, что еще можно сделать с RBL с точки зрения стороны, связанной договорными обязательствами. По-моему, RBL занимают прекрасное место в экосистеме, учитывая их уникальное пространство для наблюдений, позволяющее им получить телеметрические данные для лучшего информирования о степени эффективности уничтожения этих базовых платформ, которые систематически поддерживают злоупотребление доменами.

Так что, надеюсь, мы сможем поработать вместе с сообществом ICANN над тем, чтобы продвинуться в этом направлении. Спасибо.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Мэтью.

Редж, хотите что-нибудь добавить?

РЕДЖ ЛЕВИ: Да. И, знаете, я согласен с мнением Мэтта: что значит «больше» в этих обстоятельствах?

Мы постоянно работаем с различными поставщиками списков блокировки, стремясь понять, можем ли мы пользоваться их услугами с учетом таких проблем, как ложноположительные срабатывания и сроки исключения ресурса из списка после принятия мер с нашей стороны, поскольку, как некоторые... как ранее указывалось во время ряда обсуждений, иногда в список блокировки домены попадают по ошибке, и необходимо понять, насколько мы готовы наказывать невиновных владельцев доменов в стремлении добраться до всех злоумышленников. Для меня важны обе задачи.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Редж.

Теперь я передаю слово Джоанне, нашему представителю At-Large — сообщества конечных пользователей. И мне

хотелось бы спросить вас вот о чем: Как вы считаете, чем поставщики списков блокировки ресурсов с плохой репутацией могут помочь конечному пользователю, который внесен в список или у которого возникла проблема со списком блокировки?

ДЖОАННА КУЛЕША: Спасибо Эл Джи. Я понимаю, что время ограничено, но позвольте мне кратко остановиться на плодотворной дискуссии, которую мы ведем.

Для записи стенограммы и перевода — это Джоанна Кулеша.

Это действительно основной вопрос, на который пытается ответить сообщество At-Large: Какое прямое влияние списки блокировки ресурсов с плохой репутации оказывают на ситуацию, в которой находятся конечные пользователи? Куда они могут обратиться, если их доменное имя было несправедливо включено в список вредоносных? То есть для нас вопрос состоит в информировании всего сообщества о результатах этого заседания, защите интересов конечных пользователей и разработке критериев составления списков блокировки ресурсов с плохой репутацией.

Мы рады возможности участвовать в обсуждениях, которые идут в палате сторон, связанных договорными обязательствами, и в GAC, о чем я пыталась кратко рассказать в чате.

Как правило, конечные пользователи обращаются к своим местным поставщикам услуг или правоохранительным органам, стремясь защитить свой домен, доменное имя, товарный знак, ресурсы и услуги, которые они предлагают. Но эти методы могут оказаться неэффективными, потому что, пройдя по цепочке списков блокировки ресурсов с плохой репутацией, конечный пользователь окажется именно в этой дискуссионной группе.

Так что для нас это двоякий вопрос. С одной стороны, мы хотим получить конкретный ответ для наших конечных пользователей о том, как они могут удалить сайт, включенный в этот список по ошибке, так как на самом деле этот сайт не используется для вредоносной деятельности.

Таким образом, обсуждение автоматического и ручного внесения в список блокировки является для нас одновременно и средством наращивания потенциала конечных пользователей, и гарантией того, что критерии внесения в список блокировки будут соответствовать их

потребностям и ожиданиям. Хотя кажется, что в данный момент, как отметил Питер в окне вопросов и ответов, больным вопросом является управление и подотчетность списков блокировки ресурсов с плохой репутацией.

Как мы поняли в результате сегодняшнего обсуждения, принимаются во внимание различные критерии. Между теми, кто предоставляет такие списки блокировки, ведутся переговоры; но нам, чтобы понять, как работает вся эта система, нужны общие знаменатели или возможности, подобные этой, чтобы лучше разобраться в том, как работает эта система, и иметь возможность внести свой вклад в ее развитие.

Итак, заниматься обсуждением критериев, которые будут использоваться для внесения определенных сайтов в список блокировки, действительно должно сообщество ICANN, в котором голос At-Large должен быть принят во внимание.

Мы слышали о спаме. Сообщество At-Large организовало вебинары, заседания, обсуждения внутренней политики для определения категорий злоупотребления DNS. Спам оказался одним из самых спорных вопросов: в одних юрисдикциях он узаконен, а в других нет.

Поэтому, что касается списков блокировки ресурсов с плохой репутацией, для нас важным элементом являются критерии их составления. Мы рады возможности участия в этих обсуждениях, а также в пленарном заседании в понедельник, где будут обсуждаться изменения в области регулирования, которые, вероятно, также повлияют на работу регистратур и регистраторов в разных юрисдикциях.

На этом я остановлюсь. Я знаю, что у нас мало времени, Эл Джи, но считаю, что эту дискуссию нужно продолжать.

Спасибо.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Джоанна. Я хотел бы задать поставщикам списков блокировки ресурсов с плохой репутацией вопрос, непосредственно связанный с заявлением Джоанны.

Что бы вы посоветовали сделать конечным пользователям, по ошибке внесенным в список блокировки, для решения этой проблемы? Карел.

КАРЕЛ БИТТЕР: Конечно, да. Я не знаю, как поступают другие. Я могу рассказать вам, как поступаем мы. У нас есть сайт с функцией

поиска, где можно выяснить... вы знаете, поскольку мы говорим о доменах, есть ли ваш домен в наших списках. Если это так, в большинстве случаев вы можете подать заявку на удаление напрямую, которая будет обработана напрямую, и в течение минуты домен будет исключен из наших массивов данных. Эти массивы данных обновляются ежеминутно.

Иногда вам придется создать заявку из-за того, что мы занимаемся сбором определенных показателей. И у нас есть люди, которые круглосуточно и без выходных обрабатывают заявки, чтобы помочь вам понять, в чем проблема, и что, по нашему мнению, необходимо сделать для исключения ресурса из списка, и человек просмотрит список, а затем либо поможет вам понять, что происходит, либо исключит домен из списка.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Карел. Бен, в вашем случае есть существенные отличия?

БЕН КУН: Интересно. В нашем случае список используется, как правило, только в течение 24 часов, поскольку фишинговые сайты отключаются от интернета. Однако мы делаем в основном то

же самое, о чем рассказывал Карел: если кто-то сообщает нам о ложноположительном срабатывании или о чем-то, что выходит за рамки нормы, вы знаете, мы внимательно изучаем это, не только причины автоматического включения в список, но и конкретную ситуацию.

Вы знаете, когда мы сообщаем о чем-то регистраторам или хостинг-провайдерам, и они нам возражают, мы относимся к этому очень серьезно и очень внимательно изучаем вопрос, чтобы не исключить из списка то, что законно признано фишинговым или вредоносным ресурсом. А если это не так, то сразу убираем его из списка. Знаете, как говорил Карел, в считанные минуты.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Бен. Из сегодняшнего обсуждения ясно, что не существует общего цикла обратной связи для сообщения об устранении злоупотребления или ложного срабатывания.

Роман, как вы думаете, хотели бы вы поработать над стандартизированным способом получения такой информации из множества источников? И что бы вы... что бы вам потребовалось... какое содействие нужно было бы вам оказать, чтобы вы ему доверяли?

РОМАН ХЬЮССИ: По-моему, это интересное обсуждение. Разумеется, у меня нет прямого ответа на ваш вопрос, но это, по-моему, был бы хороший способ... оказать содействие и, да, завоевать доверие в сообществе благодаря чему-то подобному. Так что над этим определенно можно поработать. Вопрос только в том, да, кто будет служить прикрытием для такой… такой вещи, будет ли это ICANN или кто-то еще. Это должны решить участники отрасли.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Роман.

Джоанна, я хочу вновь обратиться к вам и задать вопрос. Это не связано напрямую со списками блокировки ресурсов с плохой репутацией, однако какие средства защиты, по вашему мнению, необходимы, чтобы регистратуры и регистраторы не превышали своих полномочий в том, что касается отключения доменных имен, о которых поступила информация, что они участвуют в злоупотреблении DNS?

ДЖОАННА КУЛЕША: Я поддержу заявление Мэтта. Это Джоанна, еще раз для протокола. Все дело в транспарентности. Чем понятнее будут критерии и чем более открытыми будут поставщики списков блокировки ресурсов с плохой репутации при

обсуждении применяемых критериев, тем легче будет среднему конечному пользователю понять процесс и высказать свое мнение.

И я твердо уверена, что именно здесь At-Large может помочь определить ожидания. Ответ мог бы носить региональный характер. Мы обсуждали это и на заседании в понедельник. Сообщество At-Large проводит кампанию по наращиванию потенциала в области борьбы со злоупотреблением DNS, которая стартует на региональном уровне. Таким образом, это действительно могут быть ответы регионального уровня от лица конечных пользователей. В разных RALO, в разных странах ожидания могут быть разными. Мы видели, какие они в Европе во время заседания в понедельник.

Но, как я понимаю, это пойдет на пользу дальнейшему развитию модели с участием многих заинтересованных сторон.

Чтобы мы смогли внести лучший вклад в это обсуждение, как подчеркнул Мэтт, транспарентность процессов, понимание принципов их работы и как всегда добросовестные действия сообщества ICANN, я думаю, помогут нам продвинуться в деле результативного развития списков блокировки ресурсов с плохой репутацией. Спасибо.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Джоанна.

Теперь я собираюсь задать вопрос, поступивший от аудитории. Он получен от Фолькера Греймана (Volker Greimann), который спрашивает: Почему так много списков блокировки ресурсов с плохой репутацией принимают сообщения, не содержащие доказательств? Без доказательств или конкретной ссылки, позволяющей проверить сообщение, слишком трудно принять меры.

И я передам слово Карелу.

КАРЕЛ БИТТЕР: Конечно, да. Итак, давайте поговорим о спаме в этом контексте. Это то, с чем я лучше всего знаком.

Мы получаем сообщения о спаме либо от корпораций с крупными ISP, в которых они раскрывают определенные характеристики спама, либо от наших собственных спам-фильтров или ловушек для хакеров, если можно так выразиться.

Спамеры стали очень хорошо встраивать всевозможные мелкие детали для отслеживания в URL-адреса, домены, изображения, в полные электронные письма. Масштаб таких

вещей, которые мы получаем, не позволяет гарантированно удалить все и при этом полностью очистить представленные нами доказательства от всего, что позволит обнаружить наши ловушки для хакеров. Таким образом, в этот момент принимается решение: раз нельзя поделиться сведениями, не защитив свои источники, то ими нельзя поделиться.

Как я уже сказал, в каждом конкретном случае мы всегда готовы работать над тем, чтобы представить людям необходимые им доказательства, если мы можем ими поделиться. Но в автоматическом режиме это просто невозможно сделать.

Чтобы дать вам представление, всего лишь одна группа запущенных нами ловушек для хакеров, получает от 2000 до 3000 писем в секунду. Мы не можем профильтровать все это, убрать все идентификаторы и убедиться, что данные, которые мы предоставляем, будут... чистыми и не позволят обнаружить источники.

Как я уже сказал, если людям, которые занимаются исправлением ситуации, нужны конкретные доказательства, то те, кто пользуется нашими данными для этой цели, знают, как с нами связаться, и могут узнать дополнительные подробности, когда это возможно.

ЭЛ ДЖИ ФОРСБЕРГ: Спасибо, Карел. К сожалению, на этом сегодняшнее заседание подходит к концу, поскольку у нас заканчивается время.

Глядя на ответы участников опроса, полученные в начале заседания, я бы сказал, что сегодня аудитория была довольно широкой. Есть те, кто не слышал о большом количестве различных видов злоупотреблений, и те, кто определенно об этом слышал. Есть те, кому не приходилось бороться со злоупотреблениями, и те, кому приходилось.

Надеюсь, некоторые из нас узнали довольно много из сегодняшней дискуссии и смогут продвинуться в своей работе, касающейся этой конкретной темы.

Я хотел бы поблагодарить всех экспертов за участие и потраченное время, персонал ICANN за неоценимую поддержку и, наконец, что не менее важно, аудиторию, которая нашла время в течение этой насыщенной событиями недели конференции сесть и послушать.

Понимание списков блокировки ресурсов с плохой репутацией, их функций, целей и способов их применения или способов связи с их составителями для исправления ошибок — очень важный шаг в определении способов работы с ними и мер противодействия злоупотреблению DNS.

Впереди долгий путь, но лично я считаю, что сегодня мы добились некоторого прогресса.

Еще раз спасибо всем за участие.

БРЕНДА БРЮЭР: И в анкете остался последний вопрос. Мы прямо сейчас его откроем. Подождите.

И этот вопрос анкеты должен быть у вас на экране. «Вы знаете, как сообщить об угрозе безопасности или предпринять другие шаги для устранения этих угроз?» Пожалуйста, ответьте «да» или «нет».

Опять же, вопрос на вашем экране: «Вы знаете, как сообщить об угрозе безопасности или предпринять другие шаги для устранения этих угроз?» Пожалуйста, ответьте «да» или «нет».

Спасибо. А я закрою опрос и сообщу его результаты.

Большое спасибо за ваше сегодняшнее участие. Объявляю заседание закрытым.

Спасибо всем.

БРЕНДА БРЮЭР: Можно остановить запись.

Спасибо всем.

**[КОНЕЦ СТЕНОГРАММЫ]**