ПЕКИН — Оперативные данные по безопасности, стабильности и отказоустойчивости (БСО) новых рДВУ
Понедельник, 8 апреля 2013 г., 15:00 – 16:30
ICANN — Пекин, Китайская Народная Республика

Дамы и господа, прошу приветствовать руководителя службы безопасности ICANN Джеффа Мосса (Jeff Moss).

[Аплодисменты]

ДЖЕФФ МОСС (JEFF MOSS): Прежде всего нам нужны микрофоны. Вот так. Хорошо. Мы начинаем. Будут представлены оперативные данные по безопасности, стабильности и отказоустойчивости новых рДВУ. Сегодня мы собираемся рассказать вам в общих чертах о том, как ICANN и расширенное сообщество изучают риски, связанные с программой внедрения новых рДВУ.

Здесь в президиуме есть несколько человек, которые намерены помочь нам в этом и изложить свое мнение и видение проблем. А затем, в конце заседания мы также собираемся попросить вас задать вопросы. И следует надеяться, что нам удастся всесторонне обсудить несколько проблем.

То есть я хочу сказать, что в конце этой встречи состоится интенсивный диалог. Поэтому, так как мы не планируем отвечать на вопросы в ходе заседания, приберегите их напоследок.

Записывайте свои вопросы. Члены президиума останутся здесь до самого конца, и тогда мы сможем обратиться к ним.

Здесь на сцене находится вице-президент по вопросам деятельности рДВУ Кристина Уиллетт (Christine Willett). С нами вице-президент IANA Элиза Герих (Elise Gerich). С нами начальник службы безопасности VeriSign Дэнни Макферсон (Danny McPherson). Директор оперативного отдела DNS в ICANN Джо Эбли (Joe Abley). С нами директор... старший директор по вопросам безопасности, стабильности и отказоустойчивости службы безопасности Джон Крейн (John Crain). С нами председатель ККБС Патрик Фальтстром (Patrik Faltstrom). С нами старший ретроспективный френолог Google Уоррен Кумэри (Warren Kumari). И с нами старший технический аналитик ICANN Стив Шенг (Steve Sheng). Вот этих людей вы видите здесь на сцене.

Я просто хочу повторить то, что нам всем известно. Основная миссия ICANN, безопасность играет очень важную роль. К этому призывает устав ICANN с поправками от 20 декабря 2012 года. И нашей миссией является координирование на высшем уровне глобальных систем уникальных идентификаторов Интернета и, в частности, обеспечение стабильного и надежного функционирования систем уникальных идентификаторов. Таким образом, если вы заглянете в наш устав, то найдете этот текст в параграфах 1 и 2 на странице 1. Это вынесено на первый план, и мы относимся к этому очень серьезно.

В качестве всемирной организации с многосторонним участием мы пытаемся способствовать безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов Интернета за счет координации, взаимодействия и сотрудничества.

И это, безусловно, ограничено функциями, выполняемыми в рамках технической миссии ICANN.

Итак, как я сказал ранее, мы собираемся сосредоточить внимание на программе ввода новых рДВУ. И если вы обдумаете это, то обнаружите здесь своего рода три роли. Первым пунктом будет то, что находится под управлением организации ICANN, область эксплуатационной ответственности ICANN. Вторым пунктом для корпорации ICANN является сообщество, к которому она обращается, фактически выполняя здесь координационную роль.

И наконец, если рассматривать мировое сообщество, здесь мы действительно пытаемся способствовать диалогу и достижению консенсуса. И все это связано в рамках нашей модели эксплуатации, координации и содействия.

Я хотел бы обратить ваше внимание на достаточно очевидный момент — нет такой вещи как стопроцентная безопасность. Вы можете разориться или сойти с ума, пытаясь достичь этого. Таким образом, ничто в Интернете не свободно от риска на сто процентов. Как же следует поступать в такой ситуации? Вы пытаетесь управлять рисками. И для профессионалов в сфере безопасности все сводится

к компромиссу между риском и вознаграждением или к компромиссу в отношении затрат.

Таким образом, частично ситуация определяется известными нам рисками, и мы разрабатываем стратегии снижения этих рисков. У нас есть планы их устранения. Мы определяем издержки, вероятность, последствия и работаем над уменьшением последствий и вероятности.

Но для неизвестных рисков нам необходимо ввести определенную процедуру. Мы знаем, что в рамках программы внедрения новых рДВУ могут произойти вещи, которые невозможно просчитать. Поэтому нам нужно быть гибкими и жизнеспособными, и мы должны разработать адаптируемую процедуру, которая поможет решить этот вопрос либо силами ICANN как единственного оператора, либо по согласованию с сообществом.

И именно по этой причине я хочу, чтобы сообщество принимало участие, поскольку при возникновении проблемы решать ее придется нам всем. Скорее всего, у ICANN не будет достаточно возможностей для решения волшебным образом всех проблем.

Система DNS, о которой мы говорим, является сложной, но изученной экосистемой. За несколько десятилетий мы накопили опыт эксплуатации системы DNS. И если вы оглянетесь назад, сообщество же испытало несколько расширений. Мы пережили добавление новых типов ресурсных записей, таких как записи AAAA, TSIG, DNSSEC, изменение протокола для EDNS0, введение ИДИ, и

делаем это в течение многих лет. И корневая система не вышла из строя после этих нововведений.

Мы также справились с переходом на... с маршрутизацией Anycast по протоколу BGP для распространения корневой зоны с целью повышения отказоустойчивости корневой системы, и мы перенесли это вместе с сообществом.

Таким образом, я хочу сказать, что независимо от того, какие проблемы возникнут или не возникнут в будущем, вместе мы перенесем их как сообщество, и справимся с ними, и будем двигаться дальше.

На этом следующем слайде вы видите обновленный вариант слайда, который показывал Фади на ежемесячной информационной телеконференции по вопросам новых рДВУ, где я в действительности хочу привлечь ваше внимание к нижней части вот здесь, своего рода кирпичной кладке БСО. И суть дела здесь в том, что на каждом уровне в ICANN мы признаем, что безопасность, стабильность и отказоустойчивость Интернета — наш миссия номер один. А все остальное строится на этом фундаменте. Поэтому мы не собираемся делать ничего, что подвергло бы риску безопасность, стабильность и отказоустойчивость DNS или систем уникальных идентификаторов Интернета. Мы не собираемся делать этого. В этой связи хочу сказать, что Кристина Уиллетт перед этим только что провела заседание по вопросу эксплуатационной готовности. И если вы не были на нем, то я хочу передать микрофон, если можно

так выразиться, Кристине, которая кратко познакомит нас с последними новостями, касающимися данного слайда.

КРИСТИНА УИЛЛЕТТ (CHRISTINE WILLETT): Спасибо, Джефф. Итак, на этом слайде отображены структурные элементы, компоненты программы ввода рДВУ, обеспечивающие эксплуатационную готовность. Она начинается с заявок, которые были опубликованы в прошлом июне. Мы провели жеребьевку для определения приоритетов. Мы находимся в середине этапа оценки и еженедельно публикуем результаты первоначальной оценки.

Если взглянуть вперед на дополнительные компоненты в направлении эксплуатационной готовности рДВУ, то мы перейдем к синим блокам, к этапу заключения договоров, когда... после того как мы окончательно доработаем и утвердим текст соглашения с реестрами. После того как кандидаты пройдут этап заключения договоров, они перейдут к проверке перед делегированием. После завершения проверки перед делегированием, можно будет сказать, что для них программа ввода новых рДВУ выполнена. Они выполнили свои обязанности в рамках этой программы. Мы высылаем уведомление кандидату и информируем IANA о том, что обработка этих заявок завершена. И мы выдаем им метку, сертификат для проверки подлинности, подтверждающий их право... возможность кандидата обратиться в IANA для осуществления операции делегирования.

Мы осуществим развертывание центра обмена информацией по торговым маркам. Система подтверждения для центра обмена информацией по торговым маркам уже функционирует. И мы обеспечим разработку и внедрение функциональных возможностей ранней регистрации и претензий, обеспечив их ввод в эксплуатацию начиная с 1 июля, в части претензий — в августе.

Одним из компонентов программы является ЕСБП, Единая система быстрой приостановки, которая будет доступна и введена в эксплуатацию к концу июля.

Система EBERO, служба резервных поставщиков конечных услуг реестра, начнет функционировать в августе. И наши инструменты мониторинга соглашений об уровне обслуживания (SLA) начнут функционировать в августе. Все это — компоненты программы ввода новых рДВУ, описанные в руководстве, которые мы создаем. Таков наш путь, наш график работ по обеспечению эксплуатационной готовности рДВУ.

ДЖЕФФ МОСС: Спасибо. Итак, после обеспечения эксплуатационной готовности и прохождения кандидатом всех этих этапов наступает время делегирования, запроса в IANA на делегирование нового рДВУ. И докладчиком по данному вопросу будет вице-президент IANA Элиза Герих, которая собирается рассказать о процедуре запросов на делегирование.

Элиза?

ЭЛИЗА ГЕРИХ (ELISE GERICH): Я хочу искренне поблагодарить Кристину и отдел новых рДВУ за выполнение всей трудоемкой работы по составлению списка. С точки зрения IANA делегирование рДВУ во многом является стандартной рабочей процедурой. Нам пришлось сделать немногое, чтобы подготовиться к приблизительно пятикратному увеличению количества рДВУ по сравнению с сегодняшним. Одной из задач было усовершенствование автоматизированной системы, которую мы сегодня используем. И она носит название системы RZM. RZM, система управления корневой зоной, была развернута в 2011 году, и мы работаем над внедрением улучшений вместе со своими партнерами по корневой зоне, NTIA и VeriSign, чтобы своевременно подготовить систему к приему заявок, когда они начнут поступать к нам в виде запросов на делегирование в корневую зону.

Еще одной вещью, над которой мы работаем, является переход от отчета-характеристики, который мы направляем, чтобы сообщить о том, что кто-либо выполнил все требования и отвечает всем критериям к подходу на основе контрольного списка. И мы очень тесно сотрудничаем с группой Кристины над тем, чтобы реализовать этот контрольный список в ходе процедуры ввода новых рДВУ.

И наконец, мы увеличили число сотрудников.

Если можно, давайте перейдем к следующему слайду.

Итак, по существу, мы... как я говорила об автоматизации, мы внедрили новый рабочий процесс, позволяющий создавать новые рДВУ. В прошлом было создано весьма небольшое количество новых рДВУ. И поэтому данный процесс никогда не считался настолько важным, чтобы его автоматизировать.

А теперь у нас есть процедура, тестирование которой завершилось на прошлой неделе, комплексное испытание вместе с нашими партнерами по корневой зоне. И мы готовы выйти на производственный режим 1 мая. Что ж, если можно, перейдем к следующему слайду.

В общем... затем я говорила о контрольном списке и отчете. В процессе прохождения кандидатами на регистрацию рДВУ процедуры оценки новых рДВУ, их заявки будут рассматриваться в ряде оценочных комиссий, на рассказ о которых сегодня Кристина потратила больше часа, и вы все теперь знаете лучше меня.

Следовательно, в любом случае вы пройдете через этот процесс. И после прохождения вами каждой комиссии в контрольном списке будет появляться маленький флажок. А когда вы все закончите и все флажки будут установлены, вы получите учетные данные, после чего сможете воспользоваться этими учетными данными (а все флажки будут доступны в режиме онлайн) и направить в отдел IANA запрос на обработку своей заявки с целью делегирования.

Можем мы перейти к следующему слайду?

Это всего лишь прототип. Это не является точной копией того, как будет выглядеть веб-сайт IANA. Если у вас действительно зоркие глаза, вы можете это прочитать. В принципе, здесь говорится о том, что внизу вы вводите свою строку нового рДВУ. Если у вас, скажем... в приведенном здесь примере используется строка .example. И под этим вы вводите полученные после завершения прохождения программы новых рДВУ учетные данные.

В этот момент вы запустили процесс делегирования. И в рамках этого процесса мы выполняем определенные действия, стандартные действия для всех ДВУ, мы в очередной раз проводим техническую проверку, чтобы убедиться в том, что ваши серверы имен действительно работают. Мы связываемся с контактными лицами, перечисленными в вашей заявке, чтобы убедиться в том, что они существуют. И это стандартная рабочая процедура.

И я хочу заверить вас, что мы готовы. Мы действительно работали в тесном контакте с нашими партнерами по корневой зоне, VeriSign и NTIA, а также с отделом рДВУ, и система автоматизации готова к выходу в рабочий режим 1 мая. Спасибо.

ДЖЕФФ МОСС: Отлично! Спасибо, Элиза.

Итак, после того как мы закончили с делегированием, я хотел бы немного поговорить о системе корневых серверов в разрезе последствий добавления всех этих новых рДВУ, которые могут появиться. И это относится к решению вопросов масштабирования,

измерения, мониторинга. И чтобы поговорить об этом, я передаю микрофон Джо Эбли, нашему директору по вопросам эксплуатации DNS в ICANN. И, как мне кажется, он собирается втянуть в это Дэнни из VeriSign.

Итак... да, мне нужно вернуться к предыдущему слайду, не так ли? Вот так.

ДЖО ЭБЛИ (JOE ABLEY): Спасибо, Джефф. Что же, здесь мы видим достаточно старый слайд, который широко используется уже несколько лет. Он получен из Cisco. Фактически он демонстрирует, что рост трафика в Интернете действительно зависит от количества ДВУ, которое у нас есть. Этот ожидаемый рост трафика не обязательно большой. Мы полагаем, что трафик на корневых серверах приводит к увеличению трафика в целом. Мы ожидаем их роста независимо от размера корневой зоны.

То, что здесь написано, достаточно трудно разобрать из зала, здесь показан десятилетний или около того рост количества операций делегирования в корневой зоне. Я прошу извинения за маленький масштаб здесь. За последние десять лет, как мы видим, было добавлено приблизительно 100 новых ДВУ — достаточно скромный рост. Этот график демонстрирует справа гораздо более впечатляющий рост, чем на самом деле. В действительности, абсолютный размер зоны все еще мал. Поэтому, конечно, существует обеспокоенность, несмотря на обширный опыт

множества операторов реестра, находящихся сегодня в зале, и количество людей, которые занимаются эксплуатацией корневых серверов и управляют намного большими по размеру зонами, чем эта, которые распространены гораздо шире корневой зоны. Безусловно, корневая зона важна. Система корневых серверов важна. Так что консерватизм важен. Нам надо убедиться, что корневые серверы сохранят стабильность.

ДЖЕФФ МОСС: Дэнни, вы считаете это достаточно точным заявлением?

ДЭННИ МАКФЕРСОН (DANNY MCPHERSON): Я, несомненно, считаю, что оно точное. Я считаю, что здесь необходимо обратить внимание на одну вещь: в течение последних приблизительно 14 лет было выполнено 67 или 68 операций делегирования, по-моему, что в среднем составляет 4 1/2 или 5 операций в год. В настоящее время мы стремимся в некотором роде надавить на педаль газа и сказать, что готовы выполнять 4 с половиной или 5 операций примерно каждые 36 часов.

И, таким образом, нам действительно необходимо осознавать необходимость перехода от традиционного темпа к новому темпу.

Если сделать шаг назад и вернуться, по-моему, в 2009 год, тогда ICANN заказала исследование, изучение масштабирования корневой зоны, в ходе которого были рассмотрены некоторые

возможности и различные последствия увеличения масштаба системы корневой зоны, а также проблемы, которые могут возникнуть в результате этого.

И возникли следующие вопросы... одной из важнейших вещей, на которую обратили внимание многие участники сообщества, стала возможность введения некоторых базовых параметров для всей системы корневых серверов. То есть определить для всех корневых серверов время задержки, количество запросов, потребительские аспекты или кто (неразборчиво) в корневой зоне. И в отсутствие указанных базовых параметров нажимать на педаль газа несколько более рискованно, чем это можно допустить.

Это выражено в документе SAC 46, в рекомендации номер 4 из документа SAC 46 говорится о необходимости системы раннего обнаружения, исследования нагрузки в результате масштабирования корневой зоны. ККСКС в связи с эксплуатацией корневой зоны ведет определенную работу в этой области, но, по-моему, здесь, безусловно, еще есть простор для улучшений.

Я считаю, что...

ДЖЕФФ МОСС: Подождите. Вы можете излагать свои мысли в течение всего заседания.

ДЭННИ МАКФЕРСОН: Извините.

ДЖЕФФ МОСС: Вы можете излагать свои мысли в течение всего заседания, не обязательно все сразу.

ДЭННИ МАКФЕРСОН: Все они имеют отношение к системе корневых серверов, к тому, что в результатах исследования масштабируемости и в документе SAC 46 содержалось требование к ICANN о том, чтобы обеспечить некоторую прозрачность в отношении технических характеристик системы целиком. И я считаю, что многие рекомендации, сформулированные ККБС и группой, занимавшейся изучением масштабирования корневой зоны, обусловливали внедрение новых рДВУ наличием такой прозрачности.

Нам обязательно нужно добиться этого, прежде чем мы полностью выжмем педаль газа. А нечто промежуточное может быть или не быть целесообразным. Однако я считаю, что сообщество, несомненно, давно признало и обсудило это.

ДЖЕФФ МОСС: Спасибо, Дэнни.

Итак, Джо, по серверу L корневой зоны накоплена некоторая статистика.

ДЖО ЭБЛИ: Да. Поэтому в ККСКС имеется предварительная совокупность показателей и параметров, которые еще обсуждаются. Я считаю, справедливо будет сказать, что большинство из них стабильно на данном этапе. Цель заключается в попытке создать совокупность показателей, которые каждый оператор корневого сервера сможет постоянно измерять и публиковать, чтобы была возможность определения долгосрочных тенденций изменения технических характеристик системы корневых серверов.

Поэтому первым этапом, как упомянул Дэнни, является установление базовых параметров, чтобы понять исходные технические характеристики системы корневых серверов при текущем уровне роста.

А затем, по мере того как мы начнем добавлять новые рДВУ, мы продолжим мониторинг этих параметров и будем выявлять все тенденции, указывающие на то, что система испытывает высокую нагрузку. Как я сказал раньше, мы не ждем возникновения высокой нагрузки. Однако это важная система. И мы гарантируем ее осторожную и ответственную эксплуатацию.

Итак, 3 апреля мы начали публиковать данные, собранные за предыдущие два месяца и на основе тех первоначальных и еще предварительных рекомендаций, автором которых является Питер Кок, представитель IAB в ККСКС.

Как я сказал, в течение некоторого времени они обсуждались в ККСКС. Здесь вы видите пример. Если вернуться к предыдущему

слайду, то там по этой ссылке на объявление можно перейти к ссылкам на статистику, которая в настоящее время обновляется еженедельно. Любой может перейти по этой ссылке и отслеживать различные аспекты роста в корневой зоне, а также различные показатели, которые ККСКС рекомендует собирать. Опять же, это только для корневого сервера L.

Корневой сервер L первым начал публиковать эти статистические данные, но нам известно, что остальные корневые серверы тоже их собирают. И мы намерены опубликовать их. У нас здесь есть пример. Итак, по-моему, когда людям обычно показывают такие графики, им достаточно трудно заметить на них какие-либо характерные особенности. Однако в действительности это данные за два месяца. И они демонстрируют время, необходимое для распространения новой корневой зоны на всю систему сервера L, которая состоит из распределенных по всему миру 300 узлов с произвольной адресацией, включая узлы, расположенные в достаточно слабо связанных с сетью областях и демонстрирующие наихудше совокупное время распространения, приблизительно равное 4 секундам. Шкала слева в миллисекундах.

Однако не вызывает сомнения, что в последующие месяцы мы увидим эпизодические всплески. Мы увидим линии, направленные вверх и вниз. Это происходит из-за того, что распределение сервера по Интернету и условия в Интернете меняются изо дня в день.

Важным моментом, касающимся этого графика, является не то, что на собранных за два месяца данных нет характерных особенностей.

Важным моментом для этого графика является отслеживание этого графика во времени при приближении первого делегирования и по мере продолжения делегирования, чтобы увидеть каким остается время распространения новых корневых зон по всему Интернету.

То есть, чтобы рассмотреть это в контексте: мы видим распространение в течение четырех секунд для зоны, которая публикуется дважды в день. То есть, по-моему, четыре секунды за 12 часов не очень плохо. Это точка, в которой мы сейчас находимся.

Вот пример из другого набора статистических данных. У нас есть два. Один соответствует техническим характеристикам корневого сервера L на основе статистики ККСКС, а другой набор отражает фактический размер корневой зоны, измеренный разными способами. Итак, на этом графике показан размер корневой зоны в килобайтах, наверное. В байтах? В килобайтах? Трудно разобрать.

Вот эта ступенька, которую вы здесь видите в июле 2010 — подписание корневой зоны. Это увеличение размера корневой зоны из-за криптографических подписей, криптографических ключей и тому подобного. Что касается размера корневой зоны, до этого мы наблюдали действительные функции. Мы можем предположить, что эта оранжевая линия сохранит свою направленную вверх траекторию, а темп будет расти по мере делегирования новых рДВУ.

Да. Я передам микрофон Джону Крейну.

ДЖОН КРЕЙН (JOHN CRAIN): Итак, я просто хотел познакомить вас вкратце с некоторыми статистическими данными, которые у нас есть и за которыми мы следим в системе корневых серверов. Существует программа, реализуемая региональным реестром Интернета в Европе под названием RIPE NCC. И это всемирная программа. ICANN с самого начала является одним из ее спонсоров.

График, изображенный выше, который вы можете видеть вон там, относится к корневому серверу L, потому что мы любим демонстрировать результаты своих собственных измерений. Однако они делают это для всех корневых серверов. И при этом оценивается время ответа на запросы к корневым серверам, то есть то, насколько быстро можно получить ответ на запрос к корневому серверу. Каждая из этих точек не является корневым сервером. Это небольшой компьютер, подключенный к Интернету, который задает вопросы. И это также можно отслеживать во времени. И все это сохраняется в базах данных. Это одно из графических представлений данных. Есть много других значений, которые они измеряют.

Таким образом, фактически в базах данных хранятся данные за несколько лет, на основе которых разрабатываются базовые показатели. Таким образом, этим занимается не ICANN или операторы корневых серверов. Этим занимается сторонняя организация. Так что эти данные находятся у нее... внизу есть URL-адрес. И конечно же, мы поделимся этими слайдами. Я сообщу

вам еще несколько URL-адресов, чтобы показать другие места, где можно получить статистику.

Следующий слайд, пожалуйста.

Итак, мы говорили о статистике корневого сервера L. В действительности, мы вам показывали форматированные данные. Об этом говорится в документе ККСКС: в каком формате следует представлять данные, чтобы обеспечить единые для всех нас возможности изучения этих данных?

ДЖОН КРЕЙН: Я не собираюсь проводить урок по корневым серверам. Все это присутствующие могут узнать другим способом.

Однако здесь указаны буквенные обозначения других корневых серверов, также публикующих статистику. Насколько мне известно, все они собирают статистические данные. Но у этих действительно есть общедоступный интерфейс, который можно использовать для просмотра данных, или можно обратиться в DNS-OARC — центр анализа ресурсов системы доменных имен, где хранится большое количество данных. Эти данные не имеют формата, указанного в документе ККСКС. Обработка не закончена, но данные там есть.

Следующий слайд, пожалуйста.

Кроме того, у нас также есть соглашения о сотрудничестве с несколькими операторами корневых серверов, не со всеми, хотя мы на самом деле сотрудничаем со всеми. Например, для

корневого сервера F у нас есть соглашение о взаимных обязанностях, и у нас в ICANN также есть письма о намерениях и соглашения о будущих действиях. Они говорят — это наши обязанности. Мы серьезно к этому относимся. И мы готовы работать вместе и выполнять эти действия. В других письмах есть только ссылки на веб-сайты, где это говорится. Они указывают на некоторые взаимоотношения с ICANN.

Следующий слайд, пожалуйста.

Таким образом, если вы не встречались с операторами корневых серверов, людьми, выполняющими эти обязанности, то могу сказать, что они действительно приезжают на конференции ICANN. Идет обсуждение более глубокой интеграции заседаний Консультативного комитета системы корневых серверов с конференциями ICANN, так что вы скоро увидите здесь больше таких людей. Но это те, кто занимается эксплуатацией. Они управляют серверами DNS и сотрудничают друг с другом на постоянной основе. Фактически, они три раза в год проводят личные встречи для обсуждения эксплуатационных вопросов.

ДЖЕФФ МОСС: Они также проводят учения для проверки своих систем реагирования.

ДЖОН КРЕЙН: Да, они действительно проводят учения. Они делают все, что можно было бы от них ожидать. Это часть сотрудничества — проведение совместных мероприятий, таких как учения. Кстати, наши друзья из VeriSign являются нашими самыми крупными партнерами в этой области, помогают нам финансировать ее и действительно выполнять технические задачи и тому подобное.

Мы были свидетелями всевозможных вещей в прошлом. Мы были свидетелями происходящих раньше изменений. Несмотря на это, Интернет, по-видимому, все еще работает. Так что это хорошие новости. Мы не ждем выхода системы из строя через сутки после ввода в эксплуатацию нескольких сотен рДВУ.

Могу я передать слово Дэнни?

ДЖЕФФ МОСС: Да, продолжайте.

ДЭННИ МАКФЕРСОН: Я хочу к этому кое-что добавить. Вы не увидели статистики корневых серверов A и J, которые являются двумя из 13 корневых серверов, находящихся под управлением VeriSign. И мы, конечно, намерены потратить вторую половину этого года на создание общедоступных веб-сайтов, содержащих эти статистические данные. Мы осуществляем интенсивный сбор этих данных.

Что касается договорных аспектов, то мы выполняем договор об эксплуатации корневых серверов, заключенный с Министерством торговли США.

Сегодня, на основе соглашения с ICANN, множества гарантийных писем, заменяющих системы обеспечения нормативно-правового соответствия... я хочу сказать, отделом безопасности VeriSign мне предоставлено 1 385 различных средств управления в восьми системах обеспечения нормативно-правового соответствия, которые постоянно контролируются и проверяются: от требующего высокой степени безопасности федерального закона США об управлении информационной безопасностью (FISMA) до американского закона о борьбе с корпоративным и бухгалтерским мошенничеством (SOX) и так далее. Они подвергаются аудиту, проверке и постоянному мониторингу. Конечно, мы все выступаем за некоторые договорные обязательства перед ICANN и, конечно, это может относиться к деятельности в корневой зоне и приемлемым значениям с точки зрения технических характеристик или параметров опубликования данных, или с других точек зрения. Я считаю, что введение этих рамок, безусловно, принесет пользу, поскольку у нас будут некоторые эталонные значения и общие методы для инфраструктуры, сбора данных и тому подобного.

ДЖЕФФ МОСС: Джон?

ДЖОН КРЕЙН: Извините, микрофон был выключен.

Итак, эти карты здесь, в действительности, представляют собой корневые сервера. Это очень похоже на последнюю карту. Все они основаны на некоторых внешних материалах, с которыми мы все знакомы — поставщик карт.

Здесь показана протяженность системы корневых серверов. Иногда слышны беспокойные голоса относительно того, достаточно ли у этой системы мощностей. У нее большая мощность. Я не могу назвать вам точную цифру, но я могу сказать, что у корневого сервера L есть 300 узлов. И (неразборчиво) мы управляем. У каждого из них достаточная мощность, чтобы справиться с ежедневной нагрузкой и достаточно много — 18 отдельных машин. И у нас есть 300 таких серверов, а у других операторов аналогичная инфраструктура. Таким образом, существует достаточно большая инфраструктура, которая постоянно модернизируется. Таково сегодняшнее состояние.

Если мы рассмотрим шестимесячный интервал, то, наверняка, увидим гораздо больше. Возможно, кто-то помнит DDOS-атаку на корневые серверы много лет тому назад, в тот момент у нас было только 13 физических узлов из-за технических ограничений.

Эта система эволюционирует. Система корневых серверов продолжит свое развитие по мере развития DNS и Интернета, и мы по-прежнему будем идти в ногу и, как следует надеяться, опережать потребности и требования.

ДЖЕФФ МОСС: Спасибо, Джон.

Итак, теперь мы собираемся перейти к другому разделу, где мы поговорим о подходе корпорации ICANN к решению проблем, о которых раньше не было известно. Это вещи, которые появляются внезапно и могут застать нас врасплох; возможно, это новая необычная проблема. И мы должны справиться с ней. Мы должны разработать план действий по ликвидации последствий.

Поэтому в данном случае мы собираемся поговорить об отчете, с которым многие из вас знакомы — SAC 57. И это действительно проиллюстрирует способ, используя который ICANN планирует... продолжает справляться с этими ситуациями по мере их возникновения.

Итак, я хочу передать слово Патрику Фальтстрому, председателю ККБС.

Патрик?

ПАТРИК ФАЛЬТСТРОМ (PATRIK FALTSTROM): Большое спасибо. Прежде чем я передам микрофон Уоррену Кумэри, который разъяснит тонкости документа SAC 57, позвольте мне немного рассказать о том, как мы создали этот отчет.

Прежде всего, в основе деятельности ККБС лежат действия, которые могут быть запущены какими-либо внешними вопросами,

полученными от Правления или от другого органа ICANN, возможно, от сообщества. Однако возможна ситуация, когда действие выполняется по собственной инициативе, если член ККБС внезапно просыпается среди ночи и начинает размышлять о чем-то.

Это один из так называемых вопросов, рассматриваемых по собственной инициативе. Итак, Уоррен, я не знаю, чем вы занимались, когда придумали это. Однако он принес это в ККБС, и мы решили, что это достаточно серьезный вопрос, который действительно следует обсудить.

Еще одной вещью, которую я также могу сказать об этом конкретном отчете, является следующая — да, нам всем известно, что вещи подобного рода следует выявлять в процессе исследования и анализа рисков, о котором мы только что слышали от других людей, однако нам всем также известно, что мы работаем с этой разновидностью вопросов безопасности, что независимо от того, насколько тщательно или подробно составлены отчеты подобного рода, независимо от того, сколько данных сопоставлено, всегда есть различного рода вещи, которые вы обнаружите потом. Поэтому очень и очень важно, чтобы была возможность действовать.

Таким образом, готовность не... не будет составлять сто процентов... сто процентов означает, что вы в полной безопасности. Необходимо иметь возможность реагировать на события по мере их возникновения.

Мы обнаружили и отразили в этом отчете один из примеров.

И третьей вещью, которую мы сделали немного не так, как обычно, было то, что мы вместо незамедлительного опубликования этого отчета передали его службе безопасности ICANN, чтобы... потому что мы сочли это серьезным вопросом, требующим от ICANN соблюдения политики распространения информации. И мы вернемся к этому и подробнее рассмотрим, какими были действия.

Итак, есть различные вещи, которые мы смогли... которые нам пришлось делать по-новому из-за этого отчета, однако уже просто на том основании, что нам удалось сделать это, я считаю... я заявляю, что сообщество действительно готово дружно двигаться вперед.

А теперь давайте дадим слово Уоррену Кумэри, и... который познакомит нас с содержанием SAC 57.

УОРРЕН КУМЭРИ (WARREN KUMARI): Отлично. Что ж, у меня много материалов для рассмотрения и мало времени, поэтому я собираюсь двигаться достаточно быстро.

Следующий слайд.

Итак, когда мы выполняем безопасное подключение SSL или TLS к веб-серверу, по сути, в тех случаях, когда адрес начинается с HTTPS, ваш браузер получает открытый ключ и использует его для шифрования. И он получает этот открытый ключ в сертификате,

который подписан центром сертификации, и подпись центра сертификации на этом по сути связывает открытый ключ с электронной персоной. Электронная персона — это нечто вроде www.example.com. И когда ваш браузер начинает его использовать, то он выполняет проверку, чтобы убедиться в правильности подписи и в том, что это подпись известного ему ЦС. Он выполняет проверку того, что сертификат еще действителен и его срок не истек, и он также выполняет проверку того, что имя, к которому выполняется подключение, идентично электронной персоне, указанной в сертификате.

Итак, когда ЦС выдает сертификат, когда он подписывает его, прежде всего ему необходимо убедиться, что сертификат выдается надлежащему лицу. Поэтому ЦС выполняет проверку следующим образом, в частности... или, как я полагаю, только для проверенных сертификатов доменов... они отправляют электронное письмо на адрес того домена, который подал заявку. Итак, это (проблема со звуком) example.com или адрес электронной почты, указанный в WHOIS, и данное электронное письмо содержит метку, а лицо, которое получило это электронное письмо, отвечает ЦС на него, и данное действие подтверждает, что оно контролирует (проблема со звуком) владеет доменом (проблема со звуком).

Есть еще один класс сертификатов, которые называются сертификатами внутренних имен серверов, и эти сертификаты предназначены только для внутреннего использования. Следовательно, имя. Они часто используются такими

компонентами, как Microsoft Exchange, Active Directory, серверами почты и множеством других компонентов (проблема со звуком). И электронная персона таких сертификатов имеет вид www.corp или www.accounting или mail.test. И малостью, которая отличает этот сертификат внутреннего имени сервера от обычного сертификата, является факт того, что эта электронная персона не попадает в ДВУ. Это означает, что вы не сможете использовать этот сертификат в Интернете, и это также означает, что ЦС не нужно отправлять по электронной почте письмо для проверки.

Итак, что же происходит, когда конечная метка в этих сертификатах внутренних имен серверов внезапно становится реальным ДВУ? То есть, что происходит сразу после делегирования?

Короткий ответ: происходят нехорошие вещи.

Итак, чтобы продемонстрировать это, я подал заявку на сертификат для www.site, и поскольку я понимаю, что такую сертификацию должно подтвердить реальное лицо, я придумал интересное имя, «Dulles Steel and Forge», которая (проблема со звуком). Следующий слайд.

А затем я отправил свою заявку в свой ЦС, и открылось небольшое всплывающее окно с текстом «Внимание: общее наименование www.site не будет функционировать в Интернете. Вы понимаете это?»

Я нажимаю «да». Следующий слайд.

А затем, три-четыре часа спустя они отправили мне по электронной почте сертификат. И вы можете видеть, что указанное там (проблема со звуком) имя мое. Субъект — www.site. Также есть два дополнительных имени или, на самом деле, это субъекты (проблема со звуком), который имеет www.site, а также просто .site. Подумаешь! У меня есть внутреннее имя сервера. Что в действительности я могу сделать с ним?

Чтобы продемонстрировать это, я создал фальшивый экземпляр корневой зоны в лаборатории, я делегировал домен .site самому себе, а затем я настроил веб-сервер (проблема со звуком) и открыл его через браузер Safari, и на самом деле я увидел пиктограмму замка, и мой браузер сообщил, что этот сертификат действительный. Я хочу сказать, что это справедливо. Он на самом деле действительный. Он работает.

Я проделал те же действия в браузерах Chrome, Internet Explorer, Firefox и Opera, а также использовал множество других сертификатов.

Ну и каковы другие последствия этого?

Итак, злоумышленник тоже может пойти и взять эти ДВУ, указанные в заявках, а затем пойти и получить сертификаты для широко известных имен в этих ДВУ. Затем он просто хранит сертификаты и ждет делегирования этого ДВУ.

Как только это произойдет, он начинает околачиваться в местном Starbucks, или кафе, или гостинице, где (проблема со звуком) имена

или (проблема со звуком) целое множество других (проблема со звуком) видов атак, и когда кто-то переходит на сайт, для которого у него есть сертификат, он демонстрирует этот сертификат, и пользователь видит пиктограмму замка, а затем злоумышленник скрывается вместе со всеми вашими деньгами или реквизитами ваших банковских счетов или с вашими куки-файлами, или с чем-то, еще, что ему удастся раздобыть.

Поэтому (проблема со звуком) консультативное заключение, и мы сделали несколько рекомендаций, которые служба безопасности должна довести до сведения форума CA/B, форума центров сертификации и разработчиков браузеров, своего рода отраслевой группы, представляющей ЦС, (проблема со звуком) политика раскрытия информации об уязвимостях, касающаяся обработки такой информации, план связи со всеми затрагиваемыми сторонами и план действий в чрезвычайных обстоятельствах (проблема со звуком), до того как мы найдем способ устранения этого.

А теперь я передам микрофон обратно службе безопасности, которая расскажет о том, как это было выполнено.

ДЖЕФФ МОСС: Спасибо, Уоррен. Я хочу дать слово Стиву Шенгу.

СТИВ ШЕНГ (STEVE SHENG): Спасибо, Джефф. Когда DNSSEC поставила эту проблему перед ICANN в начале января, мы отнеслись к ней очень серьезно. Поэтому вскоре после проведенного в формате телеконференции брифинга мы сформировали группу по предупреждению последствий, в состав которой вошли представители нескольких отделов.

И эта группа по предупреждению последствий регулярно проводила совещания, на которых планировала меры предупреждения последствий в ожидании отчета ККБС.

Таким образом, в период с января по февраль мы сделали следующее. Мы провели несколько телеконференций, в том числе с участием председателя форума CA/B и представителей крупных ЦС, предупредили их об этой проблеме, и они предложили нам выступить на своей февральской конференции. Там мы официально познакомили их с этой проблемой.

Они тоже отнеслись к ней серьезно. Я хочу отметить, что эта проблема не является новой. На данную проблему сертификатов внутренних имен Фонд электронных рубежей указывал центрам сертификации еще в 2010 году.

Я считаю, что в данном случае они действовали очень быстро. Они подготовили Бюллетень 96, о котором я расскажу на следующем слайде.

То есть 20 февраля стало важной датой, они провели голосование, и Бюллетень 96 был принят. Это существенно сократило область уязвимости.

После этого ККБС доработал свое консультативное заключение, и 15 марта, в соответствии с рекомендацией ККБС, мы уведомили об этой проблеме всех кандидатов на регистрацию новых рДВУ.

Следующий слайд, пожалуйста.

Предыдущий. Хорошо. Бюллетень 96 фактически рекомендует центрам сертификации немедленно прекратить выпуск внутренних сертификатов, а в течение 30 дней с момента одобрения корпорацией ICANN эксплуатации нового рДВУ... это означает подписание корпорацией ICANN договора с оператором... ЦС обязан прекратить выпуск данного вида сертификатов, а в течение 120 дней после опубликования договора центры сертификации обязаны аннулировать все сертификаты, которые оканчиваются суффиксом нового рДВУ.

Итак, действуя в соответствии со своими обязательствами, мы создали службу уведомлений для ЦС, чтобы сообщать им о том, на какие строки подаются заявки, и всегда, когда будет подписан новый договор между ICANN оператором ДВУ, мы будем отправлять центрам сертификации уведомление, чтобы... помочь им соблюдать указанные сроки.

Следующий слайд.

Еще остаются некоторые риски, связанные с этой проблемой, и на нескольких следующих слайдах мы планируем рассказать о том, какие это риски и как мы планируем их снизить.

И мы хотим предложить сообществу также направить нам свои замечания.

Итак, первый риск заключается в том, что согласно нашим ожиданиям большинство центров сертификации будет соблюдать требования, изложенные в Бюллетене 96, но не все ЦС являются участниками форума CA/B. Поэтому существует возможность того, что некоторые ЦС не будут соблюдать требования Бюллетеня 96 до того момента, когда этот документ официально станет (проблема со звуком) требованием. Например, так будет в случае WebTrus для Северной Америки и ETSI для европейских стандартов — основные разработчики браузеров используют эти стандарты для... все центры сертификации включают их в свой список корневых зон.

Таким образом, мы... стратегия наших действий в этом случае состоит в том, чтобы сообщать об этом риске и активно работать с теми сторонами, которые могут внести необходимые изменения.

Одной из таких сторон, с которой мы активно работаем, являются разработчики браузеров — мы пытаемся убедить их действовать с упреждением событий и потребовать от ЦС соблюдения Бюллетеня 96.

Мы считаем, что риск при этом снижается.

Следующий слайд.

Вторым оставшимся риском по множеству причин, и я считаю, что главным образом по причине низкой производительности, является наличие версий некоторых браузеров, не выполняющих... не проверяющих в режиме реального времени факт аннулирования.

Таким образом, возможна ситуация, когда ЦС аннулирует сертификат, но если браузер не поддерживает проверку аннулирования в режиме реального времени, все еще сохраняется период уязвимости, в течение которого сертификат... все еще отображается как действительный.

Наша стратегия состоит в том, чтобы сообщить об этих рисках. Мы уже сообщили об этом разработчикам браузеров и обсуждаем с ними то, каким образом лучше всего решить эти проблемы.

Предлагается множество вещей, и мы активно обсуждаем это с ними.

Следующий слайд.

И в-третьих, все еще может существовать период уязвимости с момента подписания договора между ICANN и оператором и ДВУ до того момента, когда оператор ДВУ активирует домены второго уровня.

Итак, на этом графике показана своего рода линия времени. Если начать... если отсчитать 120 дней, то есть приблизительно 17 недель, и при этом подписание договора соответствует нулевой

неделе. После этого мы переходим к проверке перед делегированием, а затем к выполняемой IANA операции делегирования, затем идет 30-дневный период уведомления о ранней регистрации, за которым следует период ранней регистрации.

Итак, по моему, все это демонстрирует, что еще может существовать окно уязвимости, и, на самом деле, по данной проблеме мы хотим... следующий слайд... получить предложения сообщества относительно того, каким образом, выступая в роли координатора, можно наилучшим способом снизить этот риск.

Таким образом, как упоминал ранее Джефф... и, по-моему, Патрик тоже... иногда невозможно заранее предвидеть все риски. Все, что вам необходимо сделать, это подготовиться к реагированию и установить процедуру, и я передаю микрофон Джеффу для рассказа об этом.

ДЖЕФФ МОСС: Спасибо, Стив.

Итак, я хотел бы, чтобы она была немного крупнее, но, по существу, это блок-схема нашей процедуры скоординированного раскрытия информации об уязвимостях, которую утвердила ICANN, а мы опубликовали в прошлом месяце, и мы применили ее к проблеме, изложенной в SAC57. Это была своего рода наша репетиция, позволяющая убедиться в работоспособности и выполнить тонкую настройку.

И в будущем мы будем таким способом раскрывать информацию об уязвимостях.

Есть несколько путей, которыми это можно сделать.

Давайте подумаем об этом в следующем ключе. Вы, как участник сообщества, можете обнаружить проблему, скажем, с корневым сервером, программным обеспечением корневого сервера, сервером имен и сообщить эту информацию ICANN.

В этом случае мы используем данную процедуру для определения того, как мы в дальнейшем будем доводить эту информацию до сведения затронутых сторон.

В другой ситуации мы, ICANN, можем являться затронутой стороной. Вы можете обнаружить уязвимость в одной из наших веб-служб или в одном из наших веб-приложений, обратиться к нам и сказать: «ICANN, я хочу рассказать вам об обнаруженной мной проблеме. Как все это будет происходить? Вы собираетесь обнародовать мое имя? Будет ли соблюдаться прозрачность?» Может быть, я не хочу, чтобы мое имя было обнародовано. То есть мы будем следовать этой процедуре при раскрытии информации о наших собственных уязвимостях.

Таким образом, это обобщенный способ уведомления затронутых сторон и взаимодействия с теми, кто, возможно, избегает прямого контакта с... с затронутыми сторонами.

Да, я вижу.

И затем достаточно новая иллюстрация. Мы опубликовали ее в нашей концепции БСО для сообщества, однако если у вас не было возможности с ней ознакомиться, то по существу здесь визуально представлено то, как... общий подход ICANN к риску и информационному обмену с сообществом, и это наш последний слайд в презентации, а теперь у всех, кто хотел задать, записывал вопросы, есть шанс спросить у нас что-нибудь.

Я знаю, что среди публики есть несколько представителей от... да, Дэнни, от...

ДЭННИ МАКФЕРСОН: На самом деле, я хотел вернуться к сертификатам внутренних имен, прежде чем мы начнем отвечать на вопросы. У меня есть комментарий к слайду 45.

ДЖЕФФ МОСС: Хорошо. Давайте вернемся. Какой слайд? Этот?

ДЭННИ МАКФЕРСОН: Вообще говоря, может быть тогда 44.

ДЖЕФФ МОСС: Этот?

ДЭННИ МАКФЕРСОН: Да.

ДЖЕФФ МОСС: Отлично. Хорошо.

ДЭННИ МАКФЕРСОН: Итак, одной из вещей, на которые я тоже хотел здесь указать... и, по-моему, Уоррен обращал внимание на этот момент в ходе собраний ОПНИ или РКК... является то, что, знаете, я не думаю, что здесь есть согласие... и Патрик, как председатель ККБС, может поправить меня, если я ошибаюсь, но я не думаю, что здесь есть согласие, насколько это приемлемо или нет в целом, и конечно, для ККБС, но не для широкого сообщества.

Кроме того, я считаю, что период уязвимости на самом деле неизвестен. В некоторых отношениях он продлится по крайней мере до 2016 года из-за большого количества приложений, как указывалось ранее, которые в действительности совершенно не поддерживают аннулирование, или из-за реальной возможности атак с применением технологии «незаконный посредник», когда злоумышленник намеренно отключает функции проверки аннулирования, и, по-моему, джентльмен из DigiCert, Джереми, указал на это ОПНИ. Возможно, он присутствует в этом зале и может выступить с уточнениями, если я не прав.

Еще одним аспектом, на который я хотел здесь указать, является то, что... и я знаю, что вы, безусловно, осведомлены об этом... то, что есть четыре вещи, которые можно сделать с риском.

Можно... можно избежать риска, можно контролировать или снижать риск, можно допустить риск и можно передать риск.

И если то, что мы здесь делаем, не решает проблему полностью, то в конечном итоге мы в одностороннем порядке передаем риск потребителю, верно? Это будут люди, выступающие в качестве потребителей в том пространстве имен, которое окажется уязвимым. Это будет, знаете ли, пример Уоррена с человеком в Starbucks, который подключается к сети, чтобы обновить свои финансовые или медицинские данные, и становится целью атаки с применением технологии «незаконный посредник» из-за этого нового пространства имен и некоторых вещей, которые мы вводим в рДВУ.

Поэтому я не считаю, что здесь есть какой-то... возвращаясь к более раннему выступлению Фади, я не считаю, что здесь есть какой-то магический ингредиент, который позволит мгновенно решить эту проблему, помимо серьезной координации действий и большой работы в сообществе.

И я считаю, что мы... знаете, стремительно продвинулись вперед в той работе, которую персонал службы безопасности ICANN проделал за три месяца, чтобы добраться туда, где... знаете, есть вещи, на которые указал Джефф. Я считаю, что это были... это были титанические усилия, которые однако все еще не привели... и, знаете, там такой огромный остаточный неизвестный риск... неизвестный, знаете, мы в конечном итоге, если мы будем

двигаться вперед с этим, перенося этот риск на потребителей, то это действительно вызывает озабоченность.

Последним моментом, на который я обращу ваше внимание, является то, что в исследовании RSST, которое выполнили Патрик и ряд других людей, а также в документе SAC45 и в документе SAC46, и в документе SAC57, и так далее, широко обсуждается вопрос междисциплинарных исследований. И во всех случаях говорится о том, что DNS позволяет пользователям получать доступ к каким-то ресурсам Интернета.

В идеальном случае это происходит безопасным, стабильным, предсказуемым и защищенным образом. И... таким образом, знаете, пользователи, как правило, не выходят в Интернет для получения доступа к содержимому DNS. Они используют эту систему, чтобы попасть в другое место. И поскольку эти зависимые системы привязывают себя к мировой системе DNS, стремясь к безопасности и защищенности, у нас возникает обязательство не вносить, знаете ли, в одностороннем порядке изменений в эту систему, не скоординировав того, что может повлиять на безопасность или удобство использования системы.

И это в некотором роде решающий момент, на который я хотел указать в данной связи, Джефф, поэтому спасибо.

ДЖЕФФ МОСС: Спасибо, Дэнни.

Я также хотел бы обратить внимание на то, что среди публики есть представители операторов других корневых серверов, представители форума центров сертификации и разработчиков браузеров CA/B, и поэтому я надеюсь на оживленную дискуссию с другими экспертами, входящими в состав нашего сообщества.

Поэтому давайте перейдем к слайду вопросов и включим левый микрофон. Пожалуйста, скажите как вас зовут, откуда вы, а затем задавайте вопрос.

ДЖЕФФ НЬЮМАН (JEFF NEUMAN): Да. Меня зовут Джефф Ньюман. Я из компании NeuStar. У меня есть вопрос к... вчера я задал г-ну Фальтстрому вопрос. По-моему, это было вчера. Я иногда путаю дни. Может быть, это было два дня назад. Проводилась презентация ККБС для Совета ОПРИ, на которой г-н Фальтстром сказал, что ККБС не рекомендовал... Правлению как консультативная группа, они не давали Правлению ICANN рекомендации задерживать или замедлять реализацию программы ввода новых рДВУ.

Комментарии г-на Макферсона создают впечатление, что вы до сих пор убеждены в наличии существенных рисков, и, по-моему, мы слышали это, поэтому я полагаю, что мой вопрос адресован г-ну Макферсону.

Есть ли... обсуждаете ли вы какие-либо конкретные предложения по снижению этих рисков? Я хочу сказать, вы обратили внимание на риски. Каким, по вашему мнению, должен быть следующий этап?

Насколько быстро вы сможете с этим справиться? И если вы начали реализацию проекта по смягчению этих рисков, что вы планируете сделать?

ДЭННИ МАКФЕРСОН: Вопрос по существу. Я бы изучил проблемное пространство, как об этом просит созданная ICANN исследовательская группа экспертов еще с 2009 года, на предмет междисциплинарных взаимосвязей.

По-моему, интересно, что в последние два-три месяца люди серьезно всматриваются и говорят: «Эй! Мы собираемся вскоре убрать шасси в этой программе ввода новых рДВУ, к каким последствиям это приведет?»; люди начинают говорить: «Ну, что это означает, если этот ДВУ делегируют и я буду его использовать внутри компании и подпишу свою сеть?» Или, знаете: «Каков совокупный уровень прозрачности в нашей системе корневых серверов и есть ли у нас возможности раннего обнаружения, которые позволят выявлять угрозы? Предполагалось ли, что это у нас будет в тот момент, когда мы уберем шасси?»

Поэтому у меня нет магического ингредиента. Я знаю, что в сообществе действительно есть много умных людей, выполнен большой объем отличной работы по согласованию действий со всеми этими зависимыми системами, которые опираются на DNS, и что, знаете, в этой сфере еще предстоит выполнить определенную работу.

Что касается сроков или чего-то помимо этого, несомненно, это работа сообщества — определять такие вещи, и есть ли... возникают ли задержки.

Но я полагаю, что для моей организации, если бы решение принимал я, то я, безусловно, учел бы последствия этого и, знаете, я лично не стал бы использовать новый рДВУ, если бы считал... знаете, что для моих операций в сфере личного здоровья или финансов, или в другой сфере, я бы не стал использовать его, если бы считал, что эти проблемы есть в инфраструктуре, которую я использую.

Я бы... я бы воспользовался чем-то более стабильным, о котором нам... нам известно, что здесь все предсказуемо, безопасно и надежно защищено. Итак, это все, что я хотел вам сообщить.

ДЖЕФФ НЬЮМАН: Патрик?

ПАТРИК ФАЛЬТСТРОМ: Да. Ну, я хотел бы внести ясность. Заданный вами вопрос был... на который я вам ответил, был двойной.

Первый вопрос: работает ли ККБС над какими-либо последующими действиями по результатам этой работы, и в тот момент времени мой ответ был отрицательным.

А второй вопрос был следующий: принимаем ли мы какие-либо меры на основании письма, полученного от VeriSign, и ответ на это был отрицательным.

ДЖЕФФ НЬЮМАН: Хорошо. Один небольшой уточняющий вопрос, если позволите.

ДЖЕФФ МОСС: Хорошо.

ДЖЕФФ НЬЮМАН: Это касается всех ДВУ, или вы опасаетесь только за их подмножество, такие домены, как .site, .corp, .home?

Я хочу сказать, я знаю, что проблему можно распространить на все, если теоретически кто-то способен это сделать, но вызывает ли это у вас реальную обеспокоенность или это касается только подмножества?

ДЭННИ МАКФЕРСОН: Я считаю, что некоторые могут оказаться более проблематичными. По-моему, не имея всей совокупности сертификатов, выданных всеми ЦС, чего вы никогда не сможете получить... ну, это будет моим предположением... вероятно, уровни риска будут зависеть от применимости этих... знаете, этих новых рДВУ.

Знаете, есть также много других зависимостей. На некоторые из них указал представитель PayPal... Билл Смит, по-моему... и есть много других. Таким образом, я... по-моему, коротким ответом будет: возможны различные уровни риска.

На самом деле, Уоррен выполнил определенный анализ, поэтому он, возможно, захочет это прокомментировать.

УОРРЕН КУМЭРИ: Пожалуй, да. Выполняя некоторый анализ SSL... извините, данных Обсерватории Фонда электронных рубежей по SSL, которые представляют собой свод сертификатов, доступных для открытого просмотра, мы заметили несколько сертификатов для .home и .corp, а также вещи, которые можно ожидать в запросах к нДВУ из корневой зоны. Кроме того, там было множество сертификатов для .ads, и мы не могли понять, к чему они относятся. В конечном итоге, выяснилось, что это были службы Active Directory. Однако на самом деле вы не смогли бы узнать это, если бы вы не видели реальных сертификатов.

Поэтому почти невозможно узнать, какие сертификаты выданы, если у вас нет репрезентативной выборки из всех ЦС.

ДЖЕФФ НЬЮМАН: А интернационализированные символы, представляют ли они такую же угрозу, или вы считаете, что это, главным образом, относится к ASCII?

УОРРЕН КУМЭРИ: Не имею понятия, но, по-моему, человек, который сидит за вами, может ответить на этот вопрос.

ДЖЕФФ МОСС: Сначала я хочу вернуться к вопросам у микрофона.

КРИС РАЙТ (CHRIS WRIGHT): Меня зовут Крис, я из компании ARI Registry Services.

Мой вопрос похож на вопрос... Джеффа, хотя, пожалуй, немного отличается.

Заседание было замечательным в том отношении, что оно ввело нас в курс проблем БСО, связанных с программой ввода новых рДВУ. Приятно видеть всю информацию, собранную воедино в одном месте и упрощенную таким образом, что она доступна для понимания.

Однако я не понял из этого заседания того, что хотел, — плана действий ICANN, начиная с данного момента, какие действия ICANN намерена предпринять или какие действия ей осталось предпринять, чтобы решить эти проблемы, каковы сроки этих действий, какие показатели будут использоваться для каждой проблемы, чтобы продемонстрировать, что мы находимся в благополучном состоянии, все под контролем и можно безопасно продолжать движение, каких конкретных целей необходимо

достичь и, в конечном итоге, какое общее влияние окажут все эти проблемы на программу ввода новых рДВУ?

Так что давайте рассмотрим это с другой стороны и, возможно, с меньшим уклоном в сторону политики, чем это сделал Джефф, какова позиция ICANN в отношении каждой из этих проблем? Придерживается ли ICANN того мнения, что каждая из этих проблем безопасности была адекватным образом решена на данном этапе и остаточный риск снизился до приемлемого уровня, позволяющего его принять или передать?

ДЖЕФФ МОСС: Итак, я начну с этого. По-моему, можно с уверенностью сказать, и поправьте меня, если я выхожу за рамки своих полномочий, но те технические проблемы, которые были подняты, достаточно хорошо изучены техническим сообществом, и ни одна из них не принесла сильных потрясений. Тем не менее я считаю, что сейчас происходит следующее: если оглянуться назад на прошедший месяц, ты вы увидите неуклонное постепенное улучшение по всем вопросам. Так, к примеру, если были опасения, что ICANN не внедрит систему уведомления ЦС о делегировании... о времени подписания договора. Несколько дней тому назад эта система начала функционировать. Были опасения в связи с тем, что не выбраны поставщики EBERO. Что же, они выбраны. И у нас есть список, при помощи которого мы отслеживаем все эти проблемы до единой, и у нас есть план исправления ситуации или реагирования на эти проблемы, и мы поочередно решаем их.

Так вот, есть области, в которых ICANN выполняет оперативные функции, где мы можем управлять своей судьбой, они входят в сферу моей компетенции, и я принимаю решения по устранению этих проблем. В тех областях, где мы сотрудничаем с сообществом, скажем, к примеру, по ситуации вокруг документа SAC 57, там мы действительно сотрудничаем в полном объеме. Стив Шенг говорил обо всей работе, которую он выполняет в рамках сотрудничества с производителями крупных операционных систем и браузеров, однако мы не сможем рассказать вам об этом, до тех пор пока эта совместная работа не придет к своему логическому завершению. Поэтому, хотя может показаться, например, что настала пауза, разработчики браузеров ничего не делают, мы придем к решению и затем объявим об этом, во многом, как и с форумом CA/B. Таким образом, это не единственный участок нашей работы. Возможно, кто-нибудь хочет что-то к этому добавить. Нет? Хорошо. Я хочу дать слово Джереми.

ДЖЕРЕМИ РОУЛИ (JEREMY ROWLEY): Джереми Роули из DigiCert — представитель центра сертификации. Я хотел бы похвалить вас, друзья, за внедрение механизма отчетности по уязвимостям, и если бы вы могли улучшить его и сделать его более доступным и наглядным, это было бы еще лучше. Я приношу извинения, я говорю недостаточно хорошо? Поскольку мы обнаружили эту проблему незадолго то того, как вы к нам обратились, и мы не были уверены, что с ней делать, поскольку в действительности это нельзя отнести к

возражениям или чему-то аналогичному. Поэтому, если у вас есть лучшее место для сообщений об этом, то я считаю, что это бы... это бы упростило выявление проблем такого рода.

Хочу ответить на вопрос предыдущего джентльмена: фактически эта проблема касается каждого рДВУ, поскольку злоумышленник может захватить любой домен, какой пожелает, при условии что ему удастся выполнить требования... выполнить требования браузера, который просто сообщает, что вам необходимо продемонстрировать свой контроль над этим доменом, а они это могут, поскольку у них есть блок с сервером, и это не рДВУ. Так что, да. Поэтому потенциально это касается всех доменов без исключения. Однако мы рассматриваем в качестве четырех наиболее проблематичных доменов .corp, .ads, .mail и .bank. У них есть эта проблема.

А затем я просто хотел коротко прокомментировать проблему аннулирования, и я считаю, что она может быть решена, главным образом, если начнется внедрение сшивания OCSP, потому что при этом невозможно блокировать реакцию на аннулирование.

ДЖЕФФ МОСС: Есть ли браузеры, использующие сшивание OCSP?

ДЖЕРЕМИ РОУЛИ: Да, я уверен, что все основные браузеры поддерживают сшивание OCSP. Это вопрос включения данного режима на клиентском

компьютере... со стороны сервера, который, я уверен, его поддерживает, этот режим разрешен по умолчанию, и в этом случае вам просто нужно включить его на Apache и Genex. Таким образом, вопрос в том, что он не включен, поэтому многие отраслевые группы сейчас продвигают это как рекомендуемое решение.

ДЖЕФФ МОСС: Так что, может быть, как средство смягчения ситуации вы можете предложить, чтобы мы впоследствии поработали с производителями серверов, чтобы они включали сшивание OCSP по умолчанию.

ДЖЕРЕМИ РОУЛИ: Это было бы замечательно. Да. Мы продвигаем это, и если другие тоже будут это продвигать, то, наверняка, все будет внедрено быстрее. И это все, что я хочу сказать.

ДЖЕФФ МОСС: Сэр.

БИЛЛ СМИТ (BILL SMITH): Билл Смит из PayPal. Да, PayPal действительно отправил в ICANN письмо о... по существу, 13 самых крупных частных доменах верхнего уровня, на долю которых приходится порядка 10% трафика запросов к корневой зоне DNS на разрешение имен.

Это существенное количество. И мы предложили не делегировать такие домены. Знаете ли, это может создать некоторые проблемы. У нас также вызывают озабоченность другие имена, но особое беспокойство — именно эти. И потом... последствия передачи риска из... ну, сегодня, по сути, из никуда — разрешение этих имен не осуществляется. Они не могут быть разрешены. Проблема не может возникнуть. А затем, внезапно мы собираемся повернуть выключатель, и 10% запросов на разрешение к корневой зоне потенциально могут быть преобразованы в неправильные адреса. Понимаете? И это... практика, которой эти частные ДВУ продолжают придерживаться десятилетиями. Так что, это... мы считаем это серьезной проблемой. В действительности, мы высоко оцениваем быстроту реагирования ICANN и форума CA/B. Однако мы обеспокоены тем, что принятые меры, тем не менее, недостаточны. И я полагаю, что мой вопрос действительно занимает заметное положение: как мы гарантируем среди всех игроков в этой области, знаете ли, и в системе DNS, и в системе центров сертификации, и во всех остальных сопряженных системах, что это будет работать. И последним моментом является следующий: это замечательно, что мы говорим о поставщиках браузеров, принимающих меры, однако они не единственные люди или приложения, которые мы используем для подключения устройств к Интернету. Поэтому у нас есть еще много вещей, о которых стоит побеспокоиться. Так что, это... это является... это является серьезной проблемой. Фактически, это проблема, которая известна достаточно давно. И, знаете, на

самом деле мой вопрос звучит так: как мы сможем избежать дублирования этих имен?

ДЖЕФФ МОСС: Что ж, у меня есть к вам вопрос, и я только... сначала позвольте мне высказать одно соображение. Еще не принято окончательное решение, как мы писали вам в своем ответном письме, ICANN все еще продолжает изучать ситуацию. Если дать свободу мысли вместо выбора из двух альтернатив, делегировать или не делегировать, вы видите какое-нибудь среднее решение? Может быть, не делегировать в течение двух лет, дать людям время на исправление ситуации?

БИЛЛ СМИТ: Ну, в таком случае я буду говорить от своего имени, поскольку знаю, что у PayPal может быть другое решение или мнение по этому вопросу. Я считаю, что ответ положительный. Я считаю, что нам нет необходимости выбирать из двух альтернативных вариантов. Однако, если мы собираемся сделать что-то, то необходимо больше склоняться в сторону отказа от делегирования и установить больший срок, по крайней мере, для этих 13 доменов, и нам нужно проявить осторожность в отношении остальных и посмотреть, что мы можем сделать. И реальная проблема, как указал Джереми, в том, что у нас нет ни малейшего понятия, поскольку мы не имеем доступа к регистрационным записям, какие сертификаты на самом деле были выданы частным ДВУ для всех этих доменов верхнего

уровня или любых других строк, которые могут там быть. Таким образом, это проблема, которая останется с нами на некоторое время, даже если мы примем меры прямо сейчас. Поэтому я... я считаю, что есть промежуточные варианты между решением не делегировать и решением делегировать сразу, но следует быть ближе к тому, чтобы не делегировать.

ДЖЕФФ МОСС: Консервативный подход.

БИЛЛ СМИТ: Ближе к консервативному подходу, особенно для таких доменов как .corp. Это целесообразно. Это проявление здравого смысла. Не регистрировать этот домен прямо сейчас. Скорее всего, 10% всех полученных запросов к корневой зоне будут адресованы этим доменам, и они не будут действительными. Поэтому если их разрешить в адреса, то эти адреса будут неправильными.

ДЖЕФФ МОСС: Верно. Я... во-первых, у кого-нибудь еще есть дополнительные комментарии к... нет? Патрик.

ПАТРИК ФАЛЬТСТРОМ: Да, я просто хочу сказать вам большое спасибо за этот комментарий, а также за... за участие в этом диалоге, потому что именно так, как вы упоминали в своем письме, что (неразборчиво)

SAC 45, который мы опубликовали 15 ноября 2010 года, когда ККБС сообщил об этих проблемах, и, да, у нас действительно состоялся диалог с Джеффом и другими о том, не является ли это причиной, по которой нам и ККБС следует переделать SAC 45 или сделать что-то другое, чтобы изучить эти проблемы в неопределенной зоне и расследовать ситуацию. Поэтому я считаю, что это действительно очень хорошо для сообщества, что все вы выходите к микрофонам, и если у вас нет времени, или вы опоздали, или что-то еще, просто попытайтесь связаться с нами, поскольку мы здесь именно для этого и вместе пытаемся решить эту проблему. Спасибо.

РУБЕНС КУЛ (RUBENS KUHL): Рубенс Кул, домен.br. Вопрос Стиву Шенгу и, возможно, Уоррену. Рассматривали ли вы возможность модификации браузеров, например введение функции анализа даты выдачи сертификата. Поскольку, если дата выдачи сертификата предшествует фактической известной нам дате делегирования ДВУ, этот сертификат является внутренним и мы можем не обращать на него внимания, поскольку теперь этот домен делегирован. Это... один из вариантов.

СТИВ ШЕНГ: Спасибо за вопрос. На переговорах с разработчиками браузеров это действительно рассматривается как один из вариантов, который, фактически, предлагается нам одним из разработчиков. Таким образом, мы работаем над вопросом технической осуществимости

этого. Потому что, знаете, тут... нам необходимо их проинформировать об этом, знаете ли, когда... когда домены будут делегированы. И, таким образом, мы изучаем возможность этого. Так что, мы... мы сообщим вам позже дополнительные сведения об этом.

УОРРЕН КУМЭРИ: Здесь надо помнить об одной вещи: огромное количество людей все еще использует IE6 в Windows XP.

РУБЕНС КУЛ: У них есть проблемы с безопасностью.

УОРРЕН КУМЭРИ: У них много других проблем. Но только вам удастся заставить людей сдвинуться вперед с конкретной даты. Есть много старых версий. Кроме того, еще не все находится в вебе. Если вы не просматривали документы серии RFC, то там приблизительно 850 ссылок на сертификаты и приблизительно 870 ссылок на TLS. Таким образом, есть все эти остальные протоколы, такие как AAA и электронная почта, и Jabber, и все остальные вещи, которые тоже опираются на сертификаты. И, таким образом, с ними та же проблема.

РУБЕНС КУЛ: Хорошо. Спасибо.

МАЙКИ О'КОННОР (MIKEY O'CONNOR): Привет, Джефф. Меня зовут Майки О'Коннор. Большинству присутствующих я известен как убежденный энтузиаст в мире рабочих групп. Однако я хочу открыть другую грань своего интереса к ICANN. Я — владелец доменного имени corp.com, и когда я включаю маршрутизацию трафика на это доменное имя, то получаю большой объем трафика. Я получаю так много трафика, что приблизительно через 20 минут я начинаю на пределе использовать линию, арендованную у дружественного поставщика услуг Интернета. И я с огромной радостью направил бы этот трафик любому, кто захочет изучить его источники. Я могу сказать вам, что это не веб-запросы. Это всевозможные виды трафика Active Directory, обмен данными между серверами, непонятные порты, безымянные порты, которые люди используют для странных вещей. Это просто устрашающий объем трафика. И это не тот трафик, который создает проблемы в корневой зоне. Это вариант трафика для .com. Поэтому трудно вообразить, что произойдет, когда вы начнете направлять трафик .corp на внешние адреса Интернета. Поэтому я просто хотел бы присоединиться к Биллу из PayPal, а кроме того, я бы также с радостью предложил свой поток данных любому, кто желает проанализировать, что в нем находится.

ДЖЕФФ МОСС: То есть вы не думаете, что это результат автозавершения .com как .corp?

МАЙКИ О'КОННОР: Нет, оказывается в большом количестве документации Майкрософт по настройке вашего сервера, доменом по умолчанию является corp.com. Итак, это просто пример того рода проблем, с которыми вы столкнетесь при вводе домена .corp, который по договоренности используется таким способом. Однако, знаете ли, в течение многих лет приложение Microsoft FrontPage, например, по умолчанию осуществляет разрешение на имя company.com, которое тоже у меня есть в настоящее время. Поэтому у меня большой опыт наблюдения побочных эффектов этого. И одним хорошим примером того, к какого рода проблемам это может привести, является следующий: когда я впервые включил почтовый сервер для corp.com, то потратил приблизительно десять минут, чтобы получить неправильно адресованную почту на ящик joecorporatefinance@sun.corp.com, в котором до этого находились еще не опубликованные финансовые отчеты, что заставило меня с криками бежать к серверу DNS и все выключать, поскольку, безусловно, это могло создать всевозможные проблемы для разных людей, в том числе и для меня. Ну, я хороший парень. Но если плохой парень сделает это, то могут произойти всевозможные вещи, знаете ли, о которых нам сейчас мало что известно.

ДЖЕФФ МОСС: Большое спасибо, что предложили это исследователям, а не организованной преступной группировке, которая, наверняка, заплатила бы намного больше, чем мы.

МАЙКИ О'КОННОР: Да. Но в любом случае, я был бы рад предложить это, со всеми необходимыми мерами предосторожности. Но я хочу подчеркнуть, что это практическая проблема. Это не что-то гипотетическое, к чему, знаете ли, можно отнестись несерьезно. Это... это большой объем трафика.

ДЖЕФФ МОСС: Спасибо. Есть у кого-либо комментарии по этому вопросу? Я обращаюсь ко всем. Нет? Хорошо.

ЭНДРЮ САЛЛИВАН (ANDREW SULLIVAN): Меня зовут Эндрю Салливан. На предыдущем заседании для нас провели презентацию по вопросам проверки перед делегированием, которая предполагает необходимость определенного взаимодействия между проверяемыми и проверяющими, поскольку, по-видимому, это не является полностью механической процедурой, которую можно пройти или не пройти. А здесь мы только что услышали о том наблюдении, что, видите ли, внезапно люди поняли, что мы через пару месяцев уже уберем шасси и, может быть, пора начать об этом беспокоиться. И мне хотелось спросить, не говорит ли полученная нами сейчас информация о том, что все немного рискованнее, чем мы думали. Мы собираемся запустить это, а люди начинают задумываться о реальных рисках, знаете ли, всего лишь за несколько месяцев до запуска. Поэтому я хочу поинтересоваться, могут ли сидящие в

президиуме... я хочу сказать, поднявшись на уровень вверх относительно этой конкретной проблемы ЦС, которая является достаточно серьезной, я хочу поинтересоваться, могут ли сидящие в президиуме что-то сказать о своего рода общих рисках в этой области и о том, не следует ли нам пересмотреть свое отношение к тому, с какими рисками связано делегирование такого большого количества новых рДВУ без учета других последствий. Спасибо.

КРИСТИНА УИЛЛЕТТ (CHRISTINE WILLETT): Я могу сказать по поводу комментария, касающегося проверки перед делегированием. Стремление к более широкому взаимодействию между проверяющими и кандидатами на этапе проверки перед делегированием основано на необходимости убедиться, что кандидаты способны представить документацию, необходимую для начала проверки. Это не связано с отсутствием автоматизации или неработоспособностью системы автоматической проверки. Это вопрос коммуникации, возможно, языковой вопрос. Поэтому наши усилия направлены здесь на расширение осведомленности и повышение ясности и конкретности требований к представлению документации. У меня нет никакой информации о том, что при автоматической проверке возникали какие-либо проблемы. Поэтому я захотела выступить относительно этой части вашего комментария.

ДЖЕФФ МОСС: Я хочу обратить внимание на то, что это не первый раз, когда мы расширяем пространство родовых доменов, это будет уже третий раз, а все эти проблемы, о которых вы говорите, существовали еще со времени добавления первого нового рДВУ в нашу систему. По-моему, сейчас просто происходит намного большее увеличение размеров маршрутизируемого пространства, чем раньше. И теперь мы вероятно делегируем такие имена, как .bank, которые для некоторых негодяев могут оказаться намного привлекательнее, чем, скажем, .info. Однако проблемы, стоящие перед нами сейчас, те же, что и были всегда. Мы просто гораздо лучше их осознаем. Дэнни.

ДЭННИ МАКФЕРСОН: Да, я хотел отреагировать на выступления Эндрю и Кристины. Мы... знаете ли, с эксплуатационной точки зрения у нашей компании огромная инфраструктура и организационные знания, связанные с эксплуатацией реестров, но мы обнаружили, что существенная часть документации для проверки перед делегированием, мягко говоря, создает для нас проблемы. Я считаю, что, на самом деле, многое из этого, скажу для тех из вас, кому это интересно, отражено в наших письмах от 8 февраля и от 18 марта, а также в обмене корреспонденцией между Акрамом и группой заинтересованных сторон-реестров, которая составила большой список соответствующих проблем; они решаются в настоящее время, однако еще остается большое количество нерешенных вопросов, например, в рамках пилотного проекта по проверке перед

делегированием. Я думаю просто делегировать зону внутри нашей компании, у нас 110 задач, которые синхронизированы с точностью до минуты, верно? Здесь нужно точно знать, что происходит с каждым аспектом. И эта строгость важна, когда мы последовательно реализуем планы развертывания и одновременно осуществляем планирование проектов для собственных внутренних операций. И поэтому мы, конечно, ждем некоторой строгости в отношении проверки перед делегированием. И, по-моему, ситуация становится лучше, и мы с удовлетворением наблюдаем за этими улучшениями, а также с нетерпением ждем новых.

В адрес Эндрю хочу сказать следующее: знаете, своего рода мета-вопрос, я определенно согласен с этим. По-моему, это просто, знаете ли, специально отступив на шаг назад сказать — здесь есть зависимость между... ну, здесь есть последствия изменений, которые мы вносим в систему, для систем, которые в действительности, знаете ли, пользователи применяют для получения доступа к информации или услугам Интернета или подобным вещам. До тех пор пока вы не отступите явно на шаг назад и не взглянете на это, вы не увидите многих вещей. И я считаю то, что мы рассматриваем, действительно артефактом. И кажется, что это происходит слишком поздно, однако это по причине того, что люди в конечном итоге сказали: эй, здесь есть последствия для использования мной этой вещи, поскольку, откровенно говоря, не все следят за работой ICANN, или DNS, или IETF, или какой-то иной организации, они занимаются своей повседневной деятельностью. Для нас и для большинства... для

многих людей в этом зале сети и DNS — основное направление работы. Это наш бизнес. Мои сосредоточены на этом. Мы заботимся об этом, уделяем внимание. Но для людей, которые, знаете, не занимаются этим, ситуация совершенно другая.

ДЖЕФФ МОСС: Джо.

ДЖО ЭБЛИ: Я собираюсь прокомментировать только один аспект масштабирования, касающийся корневой системы. По-моему, важно обратить внимание на то, что в прошлом у нас были гораздо более крупные структурные изменения. Что мы собираемся сделать — это увеличить корневую зону до размера, который является большим в относительных величинах, но в абсолютном выражении очень мал. Мы не ведем речь о добавлении новых ресурсных записей, мы не ведем речь об изменении основного интервала ответа, мы не ведем речь об изменении протокола и возврате подписей или о чем-то еще аналогичном. Мы говорим об обычных деловых операциях в корневой зоне, размер которой немного больше. Если мы представим, что корневая зона находится здесь и заканчивается вот тут, то мы, сидящие в этом зале, уже имеем широкий опыт работы с доменом .info, который находится вот здесь, и с доменом.org, который где-то здесь. Все используют один и тот же протокол. Все используют одно и то же программное обеспечение. Итак, снова повторю, я считаю это важным, я считаю,

что Дэнни, конечно, согласится, что мы принимаем все меры предосторожности, необходимые для установления базовых значений, их измерения и отслеживания изменений в рабочих характеристиках по мере роста корневой зоны. Я полагаю, что изменения в системе обслуживания корневой зоны в действительности окажутся очень скромными. Мы здесь слышали другие вещи, которые не относятся конкретно к корневой зоне, но, знаете ли, одной из вещей, над которыми мы работаем, является эта очень важная система. Я считаю, знаете ли, что мы обнаружим... Дэнни, безусловно, может это прокомментировать, но я считаю, что реакция системы на этот предполагаемый рост будет пренебрежимо мала.

ДЖЕФФ МОСС: Патрик, а затем Уоррен.

ПАТРИК ФАЛЬТСТРОМ: Да. Просто потому что... с другим (неразборчиво) я тоже занимаюсь эксплуатацией корневого сервера I, и позвольте мне дополнить выступление Джо, поскольку мы управляем не только корневой зоной, но также несколькими нДВУ, которые... все они невообразимо крупнее корневой зоны, но это не создает абсолютно никаких проблем.

ДЖЕФФ МОСС: Уоррен.

УОРРЕН КУМЭРИ: По существу, я хочу отреагировать на то, что сказал Джефф: да, мы уже запустили несколько рДВУ раньше. Однако, когда мы делали это, то часто сталкивались с разного рода проблемами. Например, у Рэма была проблема с доменом.info, когда после ввода в эксплуатацию этот домен фактически не признавали. И представляется, что обеспокоенность, которую мы сейчас наблюдаем, вызывает, на самом деле, взаимодействие между самой DNS и другими системами. То есть, необходимость своего рода междисциплинарных исследований, которые предлагает провести ККБС.

ДЖЕФФ МОСС: Выражаясь языком ICANN, это проблемы повсеместного признания?

УОРРЕН КУМЭРИ: Ну, это только часть той проблемы .info, о которой говорил Рэм. Но это также в большей степени взаимодействие между DNS и приложениями, использующими эту систему. Так что, да, это был вопрос повсеместного признания, но также и своего рода проблема обмена данными с приложениями. И я считаю, что вопрос повсеместного признания сейчас можно считать близким к решению, но в большей степени остается проблема того, что другие компоненты, опирающиеся на DNS, окажутся в плачевном состоянии.

ДЖЕФФ МОСС: Ну, в этих ситуациях, по-моему, вы можете рассчитывать на то, что станете свидетелем все более активной деятельности ICANN в роли координатора, так как мы не контролируем вопросы разрешения имен в python или поиска имени приложением Майкрософт. Но мы, безусловно, обратимся к ним и скажем: мы обнаружили здесь проблему, и было бы замечательно, если бы вы решили ее, и у нас есть эксперты, готовые потратить свое время на то, чтобы помочь вам. При этом я считаю, что теми вещами, которыми ICANN управляет и на которые оказывает прямое влияние, мы занимаемся, вы увидите, что мы все больше и больше усиливаем свою работу в качестве координатора и партнера. Извините. Сэр.

ПОЛ СТАХУРА (PAUL STAHURA): Да, меня зовут Пол Стахура. Я из компании Donuts. И я с интересом прочитал отчет ККБС, в котором упоминалось исследование, выполненное, по-моему, в 2009 или 2010 году. И затем я...

ДЖЕФФ МОСС: Отчет по данным SSL Обсерватории EFF?

ПОЛ СТАХУРА: Да. И я подумал, что это достаточно старые данные. Знаете ли, потому что сейчас 2013 года — это было четыре года тому назад.

ДЖЕФФ МОСС: Да. Они просто не обновлялись.

ПОЛ СТАХУРА: Поэтому я выполнил одно исследование.

ДЖЕФФ МОСС: Хорошо.

ПОЛ СТАХУРА: И я здесь, чтобы сообщить вам о результатах. Итак, мы рассмотрели... мы рассмотрели зоны .com и .net, мы взяли каждое имя в этих зонах и затем проанализировали каждый сервер, на который указывает это имя, и мы обнаружили 25 миллионов сертификатов. Мы просмотрели каждый из этих сертификатов и выяснили, какие метки доменов верхнего уровня они содержат. И мы обнаружили среди этих 25 миллионов сертификатов 51 новый... новый рДВУ, предлагаемый к регистрации в этом раунде. 51 ДВУ был обнаружен в этих 25 миллионах сертификатов. И мы также пришли к выводу... мы обнаружили, что самым крупным из них был .corp, в полном соответствии с опубликованными результатами исследования. А затем мы рассмотрели поддомены, которые были указаны в домене .corp, и мы обнаружили 102 уникальных поддомена в этом гигантском пространстве возможных имен .corp, 102 поддомена. И, кстати, домен .home был вторым с 42 уникальными поддоменами. Номером 3 был .offline. Номером 4 был .inc и так далее. Итак, у меня здесь также есть список

поддоменов .corp. В домене .corp мы обнаружили, например, park .corp, digi love .corp. Вы знаете, там было 102 поддомена. И почему бы нам просто не заблокировать их на некоторое время, может быть, до этого «несчастного» 2016 года, как предложил представитель VeriSign. Мы просто заблокируем эти поддомены, независимо от того, кто получит домен .corp, нам не придется блокировать все пространство имен .corp. Сейчас мы можем прекратить выдачу этих сертификатов, а затем заблокировать некоторые до определенного момента в будущем?

ДЖЕФФ МОСС: Спасибо.

ДЭННИ МАКФЕРСОН: Я могу ответить?

ДЖЕФФ МОСС: Да.

ДЭННИ МАКФЕРСОН: Итак, Пит?

>> Пол.

ДЭННИ МАКФЕРСОН: Интересным артефактом являются данные документа SAC 57, в котором было указано 37 000 сертификатов по состоянию на 2010 год. По-моему, это замечательно, что вы действительно обновили его. Я был бы рад увидеть эти результаты опубликованными где-нибудь.

>> Хорошо, я отправлю их.

ДЭННИ МАКФЕРСОН: Однако я хочу указать на одну вещь: на самом деле, это сертификаты внутренних имен и, на самом деле, их не предполагается использовать в Интернете, верно? Таким образом, обнаруженные вами в Интернете сертификаты — это те, утечку которых в Интернет допускают люди. Поэтому данное количество представляет собой самую нижнюю границу, и следует ожидать, что у людей, которые правильно настроили конфигурацию своих систем, количество сертификатов на порядок больше. Поэтому, не имея доступа ко всей совокупности сертификатов ЦС, невозможно оценить, какие сертификаты были выданы и для каких потоков.

>> Я согласен с этим, но размер выборки достаточно велик.

ДЭННИ МАКФЕРСОН: Для внутренних сертификатов, попавших в Интернет, это совершенно верно. Безусловно.

ДЖЕФФ МОСС: Джереми.

ДЖЕРЕМИ РОУЛИ: Да. Я хочу сказать, что проблема, на которую указал Билл Смит, связана с проблемой ЦС, но отличается от нее в том плане, что большая часть этих доменов... множество этих сетей настроено таким образом, что они являются внутренними, поэтому операция разрешения в этих сетях не будет выполняться даже после включения разрешения доменов. Я хочу сказать, что это внутренние сети. Поэтому в Интернете возникнет много конфликтов со всеми этими настроенными внутренними серверами и тому подобными вещами. Люди, собирающиеся пойти в кафе и думающие, что они попадут на почтовый сервер .corp, в конечном итоге неожиданно попадут в какой-то новый рДВУ. У нас будет много проблем подобного рода. И это отличается от проблемы... сертификатов, которые выданы на эти имена. Потому что мы можем... центры сертификации могут позаботиться о решении проблемы сертификатов, но я хочу знать, что сделано для того, чтобы связаться со всеми этими сетями, настроившими свои... поставившими в центр всей своей деятельности эти внутренние сети, чтобы они изменили конфигурацию своих сетей и не создали всех этих проблем. И я не уверен, что в этой области велась какая-либо

работа по привлечению к сотрудничеству. И вы указали на это в своем отчете, однако обратились к нам, к центрам сертификации, а необходимо привлекать к сотрудничеству их. Вы что-нибудь сделали в этом направлении?

ДЖЕФФ МОСС: Кто-нибудь хочет ответить на этот вопрос? Патрик, а затем я продолжу.

ПАТРИК ФАЛЬТСТРОМ: По-моему, вы указываете на очень актуальную проблему, и даже если один из этих... один из этих доменов действительно имеет только внутреннюю сеть, именно так, как вы говорите, конечно, может возникнуть ситуация, когда результаты будут отличаться, в зависимости от разрешения домена внутри или снаружи этой внутренней области, что касается только того, находитесь ли вы вне своей корпоративной сети, но также и того, к примеру, входящим или исходящим является ваше VPN-соединение, и это иногда может привести к непредсказуемым результатам. Поэтому данный вопрос... мы, безусловно, рассматриваем в ККБС в настоящий момент, но он не является... как я сказал ранее, он не является выбранным нами направлением работы. Однако, учитывая состоявшуюся здесь дискуссию, он вполне может стать тем вопросом, который приведет к срабатыванию одного из этих триггеров, фактически обеспечивающих нас работой.

СТИВ ШЕНГ: На самом деле, я считаю, что одна из рекомендаций в документе SAC 45 предусматривала реальное привлечение к сотрудничеству тех, кого это может затронуть, и, по-моему, этот вопрос остается открытым.

>> Я только хочу сказать, что вплоть до 2011 года в документации действительно содержалась рекомендация использовать эти внутренние имена серверов для различных вещей, таких как BlackBoard и Exchange, поэтому просить людей... причиной, по которой 2016 год был выбран форумом CA/B как срок износа, полного износа этих вещей, является то, что к нам обращается много клиентов, особенно в сфере образования, которые говорят о том, что не могут внести эти изменения до указанного срока, поскольку им необходимо время для получения денег на модернизацию своих сетей, обучения своих сетевых операторов и тому подобного. Поэтому мне нравится идея не принимать решения на основе выбора одного из двух вариантов, а сказать: да, мы можем делегировать вам этот домен, но он будет делегирован в 2014 или 2015 году, когда мы... когда у нас появится возможность избавиться от этих сертификатов имен внутренних серверов, и нам известно, что... центры сертификации не выдают их уже в течение двух лет, так что проблемы больше не существует. Вы даже можете настроить браузер так, чтобы все сертификаты, выданные до этой даты, не считались заслуживающими доверия. И это дает всем время для изменения... для этого перехода.

Когда клиент приходит к вам и говорит: «Срок действия моего сертификата истекает через два месяца. Я хочу купить новый», — вы, по сути, выполняете работу по привлечению к сотрудничеству, отвечая: «Извините, сэр. Вы больше не сможете его купить. Вам необходимо составить план».

>> Это было утверждено в 2011 году, требование, чтобы все ЦС одновременно попытались смягчить эту проблему. Однако обычно они обращаются к вам приблизительно за два дня до истечения срока действия сертификата. И это обычно выглядит так: «Вот мерзопакость! Мне нужно получить новый сертификат для своего сервера, в противном случае вся деятельность станет небезопасной». Поэтому мы выдаем им сертификат на год или около того.

ДЖЕФФ МОСС: То есть вы с ними контактируете постоянно?

>> Да. В 2011 году было введено требование ко всем ЦС вести такую разъяснительную работу, чтобы они отказались от использования этого имени.

ДЖЕФФ МСС: Хорошо. Уоррен.

УОРРЕН КУМЭРИ: Однако мне следует также упомянуть, что побудить кого-то изменить то, что необходимо для признания имени сервера полностью отвечающим требованиям, гораздо проще, чем изменить всю их остальную структуру для его переименования. К примеру, присвоить компьютеру имя mail.corp, а затем получить сертификат для mail.corp, выданный food.com, — это отличается от повсеместного изменения.corp. Таким образом, это подмножество проблемы.

>> Фактически, форум CA/B провел исследование причин, по которым люди используют это, результатами которого, возможно, я могу с вами поделиться. Я попробую получить на это разрешение. Их результаты очень интересны. Многие считают, что эти имена внутренних серверов обязательны для использования. Они не понимают, что могут использовать FTD, и не знают, как это сделать.

ДЖЕФФ МОСС: У нас есть время еще для одного вопроса.

КРИС: Это снова Крис. Возможно я немного зачастил. Однако я хочу попросить вас обобщить для меня перечень действий, которые в результате этого, согласно вашим ожиданиям, должно выполнить сообщество? И какие действия собирается выполнить ICANN? Фади

во время выступления сказал, что остановит программу, если возникнут опасения в отношении безопасности и стабильности. И очевидно, что в этом зале находится много людей, у которых есть такие опасения, но они не желают останавливать программу. Поэтому как мы будем решать эти вопросы? Как ICANN намерена решать эти вопросы и какими действиями сообщество может вам помочь?

ДЖЕФФ МОСС: Кто-нибудь хочет прокомментировать или я отвечу на этот вопрос? Да, у меня возникло чувство, что вы это скажете. Поэтому, как я упоминал раньше, мы отслеживаем все риски, о которых нам сообщили, а также те риски, которые мы выявили внутренними силами, не прибегая к помощи сообщества. И мы постоянно анализируем возможные пути их снижения. Если мы встретимся с такой проблемой, как выдача сертификатов для внутренних серверов, которая приведет к практическим и масштабным последствиям, то мы сделаем паузу.

Например, если бы мы не могли сотрудничать с форумом CA/B, если бы мы не смягчили эту проблему, это была бы достаточно серьезная проблема, которая заставила бы нас серьезно задуматься об изменении программы. Поэтому нам необходимо применять индивидуальный подход.

А теперь о том, что мы ждем от сообщества: если задуматься о характере проблем, которые мы обсуждаем, то проблема

внутренних сертификатов является симптомом более широкой проблемы расширения адресного пространства корневой зоны. И я убежден, что никто из сидящих в президиуме экспертов не сможет перечислить все возможные проблемы. Однако люди в сообществе, которые постоянно работают над этим, может быть, вы можете описать ситуации, о которых нам необходимо знать. Поэтому я прошу вас, и это — наш призыв к сообществу, помочь нам выявить все остальные проблемы, о которых вам, возможно, известно. Я не хочу, чтобы кто-то сказал: «Ну, да. Я знал об этом в течение пяти лет», а потом рассказал бы нам об этом за две минуты до ожидаемого перехода в рабочий режим.

Поэтому, знаете, если вам необходимо использовать нашу процедуру скоординированного раскрытия информации, пожалуйста, сделайте это. Если вы захотите мне позвонить в частном порядке, назвавшись вымышленным именем, сделайте это. Но мы не собираемся ни от чего отворачиваться и не собираемся ничем пренебрегать до тех пор, пока не изучим это.

КРИС: Понял. Итак, исходя из формулировки, которую вы только что использовали, могу я уйти отсюда с пониманием того, что, по мнению ICANN, рассмотренные здесь проблемы надлежащим образом решены?

ДЖЕФФ МОСС: Я бы сказал, что ни одна из проблем не вынуждает нас прекратить программу, потому что все они решаются прямо сейчас.

ДЭННИ МАКФЕРСОН: На самом деле, я как частное лицо и как оператор не согласен с этим. Я считаю, что имеются существенные остаточные риски, которые в одностороннем порядке переносятся на пользователей и потребителей Интернета. И нам необходимо оценить последствия этого. Я хочу сказать, что если оглянуться назад, то одним из обещаний в рамках программы ввода новых рДВУ было следующее: эй, у нас могут быть рДВУ, которые более безопасны, которые функционируют более безопасным образом. Это обещание стало противоположностью. Я прошу ICANN рассмотреть данный аспект. И я знаю, что мы стремительно продвинулись относительно того этапа, на котором находились раньше. Но я не считаю, что сделанные к настоящему моменту заявления и выполненные действия надлежащим образом устраняют эти уязвимости.

ДЖЕФФ МОСС: Так какая... скажите сообществу, какая проблема заставляет нас остановить программу?

ДЭННИ МАКФЕРСОН: Любая из перечисленных и, безусловно, все они в совокупности. Ни одна из этих проблем не решена. Имея... я позволю выступить другим членам президиума... я знаю, что уже выступал с этим

заявлением, но у нас состоялась 90-минутная дискуссия о том, что механизм аннулирования не работает. Это может произойти после аннулирования. Знаете, что касается других пространств имен, как насчет этих последствий? И, в конечном итоге, мы просто не можем как сообщество, имеющее обязательства и обязанности в отношении DNS и зависимых систем пользователей DNS, в одностороннем порядке передать риск этим потребителям.

ДЖЕФФ МОСС: Что касается вашего примера OSCP, если браузеры начнут разрешать проверку аннулирования OSCP, если на серверах этот режим будет включен по умолчанию, то это будет принципиально иная ситуация, а не та, которая у нас есть сегодня. Правильно? Так что эта не та ситуация, в которой нет средств для снижения риска. Средства для снижения риска есть. Наша трудная задача состоит в том, чтобы сделать это режимом работы серверов по умолчанию, а не, знаете... Стив?

СТИВ ШЕНГ: Дэнни, для протокола, я не согласен с тем, что режим аннулирования не работает. Спасибо.

УОРРЕН КУМЭРИ: Таким образом, я не думаю, что мы сможем устранить здесь все риски. DNS — большая, сложная и взаимозависимая система. И, когда вы вносите в нее изменения, что-нибудь где-нибудь пойдет

не так. Мы были свидетелями того, как после развертывания все умирало. Мы были свидетелями того, как все ваши серверы имен попадают в черный список, потому что кто-то заблокировал конкретные имена. Мы должны принять решение: какой риск можно при этом допустить, и кто на самом деле возьмет на себя этот риск? Кому вы передаете этот риск? И готовы ли они принять его, и находятся ли они в выгодном положении, для того чтобы принять этот риск?

ДЖЕФФ МОСС: У кого-нибудь еще есть комментарии? Если нет, то мы перейдем к закрытию заседания. Элиза? Джон? Нет? Хорошо.

Это наше инаугурационное заседание. Если сообщество... если вы сочли его полезным, я буду рад проводить его в будущем на каждой конференции ICANN. Я просто интересуюсь. Прошу поднять руки тех, кто счел это полезным? Безусловно, мы можем доработать процедуру и, может быть, собирать вопросы заранее, чтобы более конкретно рассматривать то, что вызывает у вас озабоченность. Отлично. Следовательно, мы можем готовиться к новой встрече с вами в Дурбане. Следует надеяться, у нас будут новости. Хорошо, Майки, поскольку мы вас любим.

МАЙКИ О'КОННОР: Я знаю. Я жду. Вот он. Я не буду поступать как он и стучать по микрофону... я знаю, что это сводит с ума тех, кто использует наушники. Видите?

Есть другая точка зрения на данный вопрос. В том смысле, что программа ввода новых рДВУ — новый продукт, который предлагается множеством поставщиков. И я... я — поставщик услуг Интернета. Я на конце указки. Потому что, когда что-то ломается, они звонят не в ICANN. Они звонят не в Donuts. Они звонят мне. И как поставщик услуг Интернета я прошу вас гарантировать мне, что ваш продукт будет работать хорошо. Потому что, когда в последний раз ваш продукт работал не очень хорошо, меня обвиняли в том, что он не работает. И мне пришлось истратить много денег на звонки в службу поддержки. Так что было бы здорово, если бы ваш продукт на этот раз работал лучше. И еще, люди, предлагающие этот продукт, очень привыкли получать большой доход от обращений к DNS. И я считаю доход прекрасной вещью.

Однако мне кажется, что этот продукт еще не вполне готов к использованию. И примеры, которые привели Билл и я относительно corp.com — это один из множества примеров. Поэтому я отношусь к тому лагерю, который говорит: давайте не будем слишком вальяжно относиться к этому и давайте возложим на людей, предлагающих этот продукт, обязанность его исправить.

Если говорить о том, кто должен вести переговоры с разработчиками браузеров, ну, я не должен вести с ними переговоры. ICANN не должна вести с ними переговоры. Это должны быть люди, которым принадлежит этот продукт, они должны попытаться сделать свой продукт хорошим и

привлекательным на рынке. Это была всего лишь шумная проповедь. Прошу прощения за это.

ДЖЕФФ МОСС: На этом, большое вам спасибо.