ICANN72 | Неделя подготовки — Знакомство с Технической группой по развитию инициативы по координации деятельности в области безопасности и защиты DNS (DSFI-TSG)
14 октября 2021 года (четверг), 13:00 – 14:00 по PDT

ВЕНДИ ПРОФИТ: на заседание для знакомства с Технической группой по развитию инициативы по координации деятельности в области безопасности и защиты DNS. Меня зовут Венди Профит (Wendy Profit) и на этом заседании я исполняю обязанности менеджера дистанционного участия.

Обратите внимание, что заседание записывается, и мы соблюдаем Стандарты ожидаемого поведения ICANN. Во время заседания будут зачитываться только те вопросы и комментарии, которые отправлены с помощью функции вебинара Q&A. Мы будем зачитывать вопросы вслух в указанное председателем или модератором этого заседания время.

На заседании осуществляется перевод на все пять языков ООН. Нажмите в Zoom значок перевода в нижней части панели инструментов Zoom и выберите язык, на котором вы хотите слушать это заседание.

Если вы хотите высказаться, поднимите руку в зале заседаний Zoom. Такая возможность предоставлена участникам группы, и координатор заседания назовет ваше имя. Прежде чем начать говорить, убедитесь, что вы выбрали язык своего выступления в

меню устного перевода, если это не английский. И еще... пожалуйста, называйте для протокола свое имя и язык. Когда будете говорить, отключите звук и уведомления на всех остальных устройствах. Пожалуйста, говорите четко и с нормальной скоростью, чтобы обеспечить точный перевод.

Для общения в чате используйте раскрывающееся меню в окне чата и не забудьте выбрать пункт «Ответить всем участникам группы и присутствующим». После этого все смогут увидеть ваш комментарий. Обратите также внимание, что в формате вебинара Zoom закрытые чаты доступны только участникам группы. Все сообщения, отправленные участником группы или обычным присутствующим другому присутствующему также будут видны организаторам, соорганизаторам и остальным участникам группы.

Чтобы вывести на экран стенограмму в реальном времени, нажмите кнопку субтитров на панели инструментов Zoom. А теперь я передаю слово Джону Крейну (John Crain).

ДЖОН КРЕЙН: Большое спасибо, Венди. Всем добрый день, добрый вечер или доброе утро! Во-первых, я хотел бы передать извинения Йорана Марби, который надеялся выступить на этом заседании, но у него, к сожалению, есть другие дела, и он попросил меня сказать несколько слов от его имени. Я Джон Крейн. Я работаю в ICANN главным специалистом по обеспечению безопасности,

стабильности и отказоустойчивости, а также временно исполняю обязанности технического директора и принимал активное участие в этой инициативе. Как многим из вас известно, безопасность, стабильность и отказоустойчивость систем идентификаторов лежат в основе миссии ICANN и занимают центральное место в нашем Уставе и во всем, что мы делаем.

Йоран примерно два года назад после серии атак спросил меня, каким образом ICANN может лучше содействовать безопасности систем идентификаторов. Разработанный нами процесс предусматривал формирование группы технических экспертов из числа тех, кто работает в сфере безопасности в сообществе ICANN и за его пределами. В начале этой недели Йоран получил от этой группы технических экспертов отчет, который мы собираемся опубликовать на сайте ICANN в начале следующей недели вместе с краткой заметкой Йорана в блоге. Я хотел бы поблагодарить группу от имени Йорана за этот усердный труд. Волонтеры работают над этой серией рекомендаций уже больше года. Я участвовал в этом лично, поэтому видел, насколько усердно трудились эти волонтеры, и мы никогда не сможем в достаточной мере их отблагодарить.

Мы как корпорация воспользуемся этим вкладом. Он станет стимулом для генерального директора, и мы внимательно его изучим. И мы предложим ряд идей о том, как можно воспользоваться этой информацией для повышения безопасности DNS. На этом я хотел бы передать слово Мерике Кэо

(Merike Käo), которая столь любезно взялась координировать эти усилия почти полтора года назад. Мерике, вам слово, пожалуйста.

МЕРИКЕ КЭО: Да. Большое спасибо, Джон. Итак, на сегодняшнем заседании — это повестка дня заседания — я очень кратко расскажу обо всей работе, которую мы проделали за последние полтора года. А затем мы перейдем к содержанию этой работы и рассмотрим векторы атак в экосистеме DNS, меры по снижению рисков и, наконец, рекомендации, а также оставим время для вопросов. В каждом разделе выступит с докладом один из членов TSG. Следующий слайд, пожалуйста. Следующий слайд.

Итак, как упомянул Джон, эта работа началась в мае прошлого года, и это была инициатива, которую возглавил и конкретизировал генеральный директор ICANN. Это было сделано во исполнение его обязательства работать с сообществом над укреплением сотрудничества и коммуникации по вопросам безопасности и стабильности. В первую очередь, работа была направлена на предоставление рекомендаций о том, что ICANN может и должна делать для улучшения профиля безопасности DNS. А также о том, есть ли что-то конкретное, чего ICANN не должна делать? Следующий слайд, пожалуйста.

Как отметил Джон, эта инициатива отчасти или даже в основном была вызвана несколькими очень изощренными атаками, которые произошли несколько лет назад. И мы осознали или

ICANN осознала, что на самом деле реагирование на часть этих изощренных атак носило спонтанный характер. Поэтому необходимо найти способ создания дополнительной структуры для реагирования на эти атаки во всей экосистеме интернета, и посмотреть, где может потребоваться новый уровень сотрудничества и понимания. Следующий слайд, пожалуйста.

На этом слайде показан общий график работы TSG. Работа началась в мае, и мы сформулировали состав TSG. Первое заседание состоялось 16 июня прошлого года. Летом работа преимущественно заключалась в определении круга задач и ключевых вопросов, на которые мы хотели ответить. Ранней осенью началась наиболее тяжелая часть работы, которая продлилась до мая этого года. Предметом этой первой части обсуждения являлись коренные причины и векторы атак. А затем мы создали список приоритетов для этих конкретных векторов атак, чтобы увидеть, какие из них более серьезные и действительно требуют внимания. Мы рассмотрели меры по снижению рисков, существовавшие на тот момент или существовавшие, но не задействованные, а также меры по снижению рисков, которые, возможно, не были приняты. Затем мы создали черновик документа. После его доработки, когда у нас уже было несколько проектов рекомендаций, мы провели технические консультации с некоторыми отраслевыми экспертами, а затем, наконец, подготовили итоговый отчет и

передали его Йорану в начале этой недели. Следующий слайд, пожалуйста.

Итак, это состав TSG. В группе девять членов. И, как видите, это группа специалистов различных направлений, обладающих обширным опытом и знаниями в области управления инфраструктурой DNS при реагировании на инциденты безопасности, общими знаниями в области безопасности, деятельности регистратур и регистраторов, деятельности регистратур национальных доменов, а также опытом работы с CDN и интернет-провайдерами. Кроме того, обладающих глубокими знаниями в области DNS и техническим опытом работы с DNS. Так что у этой группы специалистов различных направлений были довольно широкие и глубокие экспертные знания. Следующий слайд, пожалуйста.

Как я уже упоминала, мы также провели технические консультации в рамках пересмотра проекта документа, и это список людей, которые представили очень обширные комментарии. Группа TSG чрезвычайно благодарна за выполненный ими углубленный анализ, благодаря которому итоговый отчет и рекомендации стали намного подробнее. Следующий слайд, пожалуйста.

Также была поддержка со стороны ICANN на нескольких уровнях. Был руководящий комитет DSFI-TSG, состоявший из четырех членов Правления и двух руководителей высшего звена. ICANN

оказала нам всестороннюю поддержку в области управления программами, коммуникаций, а также поделилась техническими познаниями в этой предметной сфере. Кроме того, у нас однозначно был превосходный технический писатель, который благодаря своим навыкам превратил очень сложную и замысловатую тему в отчет, который вы с легкостью прочтете после его опубликования. Следующий слайд, пожалуйста.

Этот слайд просто показывает широту и глубину многогранной экосистемы DNS. Ожидалось, что работа продлится год, но фактически на нее было потрачено полтора года. Она выполнялась на 100% виртуально, что создавало свои проблемы. И я лично хочу поблагодарить каждого члена TSG и персонал службы поддержки ICANN, потому что для получения окончательного результата мы провели множество заседаний, а также семинаров, которые длились по два или три часа каждые две недели. Это очень сложная тема. Но опять же, я очень горжусь результатом нашей работы. Поэтому давайте без лишних слов приступим к обсуждению сути всего этого и начнем с атак. Следующий слайд, пожалуйста. Гэвин, приступайте.

ГЭВИН БРАУН: Да, разумеется. Спасибо, Мерике. В этом разделе презентации мы поговорим о некоторых рассмотренных нами векторах атак, а также о методологии, которую мы использовали при их анализе. Давайте перейдем к следующему слайду.

Этот слайд призван проиллюстрировать — в том же смысле, что и слайд, который только что показала Мерике, — глубину и широту или масштаб рассматриваемых нами систем с точки зрения угроз и векторов атак на эти системы. Итак, мы рассматриваем... вы увидите и сторону DNS, и сторону обслуживания. Таким образом, на этой диаграмме показаны элементы, существующие как на маршруте разрешения DNS от stub-резолверов до авторитативных серверов, так и на стороне обслуживания. Сюда относятся конечные пользователи как владельцы доменов, системы, с которыми они взаимодействуют в рамках предоставления доменных имен, протоколы связи между регистратурами и регистраторами, а также посредники, такие как реселлеры. Цель состояла в том, чтобы охватить все эти различные системы и рассмотреть всевозможные векторы атак, которые могут угрожать этим системам. Следующий слайд, пожалуйста.

Итак, как показывает мой опыт, пройденный нами процесс очень похож на анализ рисков в том отношении, что мы рассмотрели различные возможные векторы атак, попытались классифицировать их и найти общие черты. То есть мы обсудили каждый из этих конкретных векторов атак, опираясь на реальные инциденты. А затем, после изучения каждого вектора атаки мы рассмотрели ряд различных вопросов о доступных мерах по снижению рисков... мы поговорим о снижении рисков чуть позже... о возможных недостатках, о том, есть ли проблемы,

связанные с неполным пониманием рисков, и является ли инфраструктура DNS, сама система DNS однозначно уязвимой для определенных видов проблем, отсутствующих в других сегментах экосистемы интернета. Следующий слайд.

Итак, на верхнем уровне мы обнаружили довольно много векторов атак, которые сгруппированы и представлены здесь. Это довольно широкие группы, и вы увидите, что некоторые из них носят весьма общий характер, поскольку участники экосистемы DNS — это организации, такие же компании, как и все остальные, и у них такие же проблемы с безопасностью, как и у всех остальных компаний, будь то банк, автомойка или оператор gTLD. Некоторые вектора атак уникальны для DNS, а также для протоколов и систем, используемых участниками этой системы. И вы увидите, что мы рассматриваем такие вопросы, как выбор TTL для записей, а также совсем элементарные вещи, например, насколько хороша политика использования паролей и так далее. Затем они были сгруппированы в векторы, описанные на следующем слайде. Давайте двигаться дальше.

То есть они были сведены в эти категории векторов атак. Опять же, мы рассмотрим некоторые из них подробнее, начиная с тех, которые в целом носят довольно общий характер. Управление учетными данными и доступом — это проблема безопасности, которая не уникальна для нашей среды. Об этом должна думать каждая компания, у которой где-то есть компьютер. То же самое с контролем доступа и авторизацией. Однако есть специфичные

для системы DNS области. Такие вещи, как подмена ресурсов, проблемы, связанные с отказом в обслуживании, а также с уязвимостями в коде и в самих протоколах. И сделанный нами при создании инфраструктуры выбор, который приводит к уязвимости систем, и вы, возможно, хотите изменить ситуацию. Можно перейти к следующему слайду?

Начнем с первого пункта — управление учетными данными и доступом. Учетные данные существуют повсюду в инфраструктуре и системе обслуживания, а также в системе авторитативных серверов. Они используются для аутентификации взаимодействия между участниками. Например, если бы вы были сотрудником регистратуры, то должны были бы использовать имя пользователя и пароль для входа в систему администрирования этой регистратуры. Если вы регистратор, то будете использовать имя пользователя и пароль для доступа к системе EPP регистратуры. Если вы сотрудник регистратора, то получаете доступ к его системам, используя свое имя пользователя и пароль, и так далее вплоть до конечного пользователя. В любой точке этой системы такие учетные данные могут быть скомпрометированы. И организации, которые занимаются управлением учетными данными, должны принимать решения о реализации политики их защиты от ожидаемых видов атак: распыление паролей, повторное использование паролей, фишинг и так далее и тому подобное. Это было основным направлением нашей работы в данной области, где мы уделили

особое внимание учетным данным владельцев доменов, аутентификации в каналах связи между регистратурами, регистраторами и реселлерами, а также угрозе использования скомпрометированных учетных данных для инициирования операций в регистратуре, выдавая себя за один из объектов в цепочке между владельцем домена и регистратурой. Следующий слайд, пожалуйста.

И вот пример проблемы ненадлежащего контроля доступа при авторизации. На самом деле здесь идет речь о захвате поддомена. То есть это сценарий, когда внутри доменного имени есть запись с псевдонимом CNAME, указывающим на какой-то другой ресурс. Это позволяет создать ситуацию, когда злоумышленник фактически может получить контроль над этим доменным именем без особой проверки того, что он действительно является лицом, которому принадлежит домен. Следующий слайд, пожалуйста.

Следующий вектор атаки связан с подменой ресурса. Это способ, с помощью которого злоумышленник может перенаправить DNS-запросы третьей стороне. Такая переадресация может иметь ряд различных последствий в зависимости от того, в каком месте системы она происходит. Иногда это можно сделать в рамках законного использования. В качестве места перехвата исходящего сетевого DNS-трафика сетью часто используются порталы авторизации, чтобы отправить пользователю форму входа на портал авторизации. Но это также может быть

результатом злонамеренных действий, например, когда активный перехват в сети используется для установки вредоносного ПО на компьютер или устройство конечного пользователя. Ряд способов, позволяющих это реализовать: подмена рекурсивного резолвера, подмена авторитативного сервера, то есть рекурсивных серверов, находящихся между конечным пользователем и полномочным источником данных зоны.

Похожие домены или копии доменов. Это несколько отличается от того, что вы могли бы сказать. Это не просто фишинг, а несколько иная схема, поскольку в данном случае целями являются пользователи инфраструктуры, а не конечные пользователи потребительских услуг. Поддельные сертификаты и манипулирование маршрутами также относятся к этому вектору атаки. Переходим к следующему слайду.

Это пример того, о чем идет речь в случае копирования доменов. Наиболее очевидным примером данной разновидности вектора атаки являются омографические атаки.

Следующим вектором атаки, который мы обсудили, были уязвимости в коде и протоколе. Нам приходится устранять разные проблемы и трудности в связи с этими двумя видами уязвимостей. Когда возникает проблема с программным обеспечением DNS, способ снижения рисков, безусловно, сильно отличается от способа устранения уязвимости протокола. Потому

что при возникновении проблем с протоколом DNS, как мы довольно давно увидели из-за ряда уязвимостей, связанных с такими вещами, как SAD DNS и, конечно же, самой известной атакой Каминского, изменение протокола влияет на функциональную совместимость. Если изменить протокол без тщательной координации со всеми различными операторами и специалистами по внедрению, возникает риск дестабилизации системы. Но такие проблемы необходимо решать, и они могут оказать негативное влияние на уязвимые системы. И, как видите, такие вещи, как отравление кэша, особенно актуальны в случае уязвимостей протокола. Следующий слайд.

Это пример того, как происходит отравление кэша. Как видите... по-моему, мы забыли нарисовать стрелки. Они видны? Вот. Они видны на следующем слайде.

Итак, если рекурсивный сервер получит запрос от конечного пользователя, который ищет icann.org, а активный злоумышленник сумеет перехватить этот запрос или отправить мошеннический поддельный ответ обратно на рекурсивный сервер до получения рекурсивным сервером ответа от авторитативного сервера, это приведет к отправке конечному пользователю поддельного ответа до того, как на рекурсивный сервер придет подлинный ответ от соответствующего авторитативного сервера. Перейдем к следующему слайду.

Выбор параметров инфраструктуры. Это решения, принимаемые оператором системы DNS или службы DNS, которые могут иметь непредвиденные последствия с точки зрения безопасности и доступности этой системы. TTL — хороший тому пример. И, разумеется, здесь мы включили в список проблем как кроткое, так и длительное время существования. Так что на самом деле речь идет об идеальном TTL: оно не слишком короткое, не слишком длительное, а как раз посередине. Есть сценарии, в которых короткое TTL полезно и уместно. И есть сценарии, в которых длительное TTL полезно и уместно. Но непредвиденные последствия действительно означают необходимость тщательной оценки рисков, позволяющей убедиться, что последствия принятых решений не догонят вас и не выйдут вам боком. И давайте перейдем к следующему слайду, чтобы как раз проиллюстрировать это.

Итак, это ситуация, когда было установлено TTL записи на авторитативном сервере. Такое TTL гарантирует, что в пределах этого TTL конечные пользователи будут продолжать получать запросы или ответы на запросы, поскольку резолвером будет предоставлена кэшированная запись. Но если злоумышленник сумеет перехватить запрос либо путем перехвата доменного имени, либо с помощью одного из других векторов, о которых мы говорили в этом разделе, то используемый в злонамеренных целях ответ будет кэширован на соответствующий период, и пользователи будут уязвимы из-за этого TTL до тех пор, пока не

истечет время существования записи и не поступит правильный ответ от авторитативного сервера. Следующий слайд.

Итак, мы обсудили саму DNS как вектор атаки. Здесь в первую очередь речь идет о таких вещах, как утечка данных и использование DNS в качестве скрытого канала. Данным DNS часто разрешено проходить через сеть и выходить из нее без фильтрации или блокировки. Злоумышленники используют эту уязвимость различными способами для проникновения в систему или кражи данных из системы. Следующий слайд, пожалуйста.

Наконец, мы обсудили отказ в обслуживании. Для любого оператора критической инфраструктуры DNS это является постоянной и первостепенной задачей и проблемой. Из-за принципов работы протокола DNS использование UDP означает, что службы DNS уязвимы для спуфинга, уязвимы для атак с усилением и отражением. Атаки типа «отказ в обслуживании» на провайдеров DNS могут нарушить работу значительно большего числа организаций, поскольку целью атаки является оператор корневого сервера, служба регистратуры или регистратора, чем прямые атаки типа «отказ в обслуживании» на конечного пользователя. Следующий слайд, пожалуйста.

На этом мы завершаем обзор векторов атак. Я передам слово одному из моих коллег, который расскажет о мерах по снижению рисков. Дуэйн?

ДУЭЙН УЭССЕЛС: Здравствуйте. Меня зовут Дуэйн Уэсселс (Duane Wessels), и я ознакомлю вас с тем разделом презентации и нашего отчета, который посвящен снижению рисков. Следующий слайд, пожалуйста.

Гэвин уже рассказал о некоторых атаках. Мы также потратили в группе некоторое время на обсуждение способов снижения последствий этих атак и придумали много разных вещей. Некоторые из них не вошли в итоговый отчет, но я расскажу именно о тех, которые в него вошли. Следующий слайд.

Группа потратила много времени на обсуждение аутентификации, и многие рекомендации и меры по снижению рисков, которые вы увидите, касаются контроля доступа и аутентификации. Итак, одной из лучших вещей, которые можно сделать для обеспечения безопасности ресурсов DNS, является использование сложных паролей. В ряде случаев слишком простые пароли приводили к компрометации. Наряду со сложными паролями можно использовать одноразовые учетные данные или многофакторную аутентификацию. И, конечно же, по мере того как учетные данные и пароли становятся все более сложными, возникает необходимость использовать какой-то менеджер паролей, который запоминает пароли вместо вас, и вам не приходится запоминать их самостоятельно.

Мы обсудили осведомленность о рисках, которая фактически означает осведомленность о различных способах взлома учетных

данных, например, путем фишинговых атак. Мы поговорили о доступности и использовании сервисов, предотвращающих применение слабых паролей. К примеру, может существовать какой-то код, информирующий вас о том, является ли конкретный пароль достаточно надежным или отвечает ли он определенным требованиям к надежности. Кроме того, есть доступные базы данных известных взломанных паролей. Никогда не следует забывать о том, что у злоумышленников тоже есть доступ к этим базам данных. Вряд ли вы захотите использовать пароли, которые уже были где-то взломаны.

Мы обсудили, какие решения по исправлению ситуации могут быть приняты в случае атаки. Наконец, мы рассмотрели способы проверки и подтверждения доменов и владельцев регистраций при отправке потенциальными клиентами заявок на обслуживание. Следующий слайд, пожалуйста.

Меры по снижению рисков с точки зрения доступности, целостности и конфиденциальности. Я бы сказал, что некоторые из них уже довольно хорошо известны. Что касается доступности, по-моему, многим известно, что единые точки отказа — очень плохая идея. И часто мы размышляем об этом применительно к сетям и сетевым услугам. Например, не размещайте все свои DNS-серверы в одной сети или в одном дата-центре. Но, конечно, вам могут прийти на ум и другие виды единых точек отказа, например, использование только одного типа программного обеспечения или даже одного типа оборудования и так далее.

Кроме того, как стало ясно многим после широко известной атаки на Dyn, при использовании вторичных служб DNS их следует распределить по разным платформам. Потому что, опять же, если у вас только одна платформа и этот провайдер выйдет из строя, то вам может не повезти.

Что касается целостности, одним из лучших способов снижения рисков конечно же, является наличие доменов, подписанных с помощью DNSSEC, и внедрение DNSSEC как на стороне публикации, так и на стороне разрешения имен для выполнения валидации. Очень хорошая идея с точки зрения предотвращения перехвата домена — блокировка на стороне регистратуры или использование ряда аналогичных средств, если они вам доступны. Кроме того, мы обсудили использование нескольких новых протоколов, таких как CDS, CDNSKEY и CSYNC, которые по сути упрощают передачу данных DNSSEC между дочерней зоной и родительской.

Что касается конфиденциальности, очевидно, что в последнее время проведена большая работа в области применения зашифрованного транспорта DNS. Мы наблюдаем все более широкое распространение этого решения, которое действительно является хорошим способом обеспечить конфиденциальность в DNS. Дальше, пожалуйста.

К другим способам снижения рисков, о которых люди обязательно должны знать, относится мониторинг. Вы можете

подписаться на услуги по защите товарного знака. Это, например, позволит вам получать уведомления о том, что товарный знак и доменное имя вашей компании зарегистрированы в другой регистратуре или другом домене верхнего уровня. Возможно, вам стоит об этом узнать. Транспарентность сертификатов — это проект, который делает запросы SSL-сертификатов доступными для просмотра. Существуют службы, которые проинформируют вас, если для вашего домена был выпущен сертификат. И если вы не подавали на него заявку, то вам, вероятно, стоит об этом узнать.

Существуют записи авторизации центров сертификации, которые можно поместить в свою зону. Такая запись CAA будет указывать, каким центрам сертификации разрешено выдавать сертификаты для вашего домена. Это хорошая идея, на которую следует обратить внимание.

Что касается RPKI маршрутизации и источников маршрутов, объявления об аутентификации могут способствовать защите ваших сетей от ложных объявлений. Вы также можете следить за ними.

Организациям, которым необходимо реализовать тот или иной способ проверки поступающих в сеть данных, вероятно, придется рассмотреть возможность применения маршрутизаторов или коммутаторов, оптимизированных для глубокой фильтрации

трафика, чтобы выполнять глубокую проверку пакетов и информировать пользователей о содержании сетевого трафика.

Что касается разработчиков ПО, мы обсудили необходимость наличия хорошей практики для всего жизненного цикла разработки программного обеспечения. Именно таков стандартный подход к разработке программного обеспечения, который включает в себя лучшие современные методы обновления, исправления и тестирования программ. И, конечно же, я уверен, что все понимают важность регулярного обновления программного обеспечения не только с точки зрения пользователя, но и с точки зрения разработчиков, чтобы поддерживать в актуальном состоянии исправления и устранять проблемы по мере их обнаружения. Дальше, пожалуйста.

Меры по снижению рисков, относящиеся к контролю доступа, включают использование так называемых архитектур доступа, основанных на поведении. Одним из примеров служит модель нулевого доверия. В последнее время она привлекает большое внимание. Всегда полезно разделять критически важные службы. Например, отделять службы DNS от служб электронной почты, от своих веб-служб и разносить по разным системам, чтобы в случае атаки на одну из служб, другие не затрагивались. Разумеется, следует рассмотреть возможность более строгого контроля доступа к тем учетным записям, которые могут требовать повышенного внимания.

В тех случаях, когда имеется возможность разделения служб, рекомендуется предоставлять доступ к службам данных только через конкретные порты DNS. Это порт 53, порт 853, у которого теперь есть TLS и, возможно, порт 443 с DNS по HTTPS. И если вы управляете резолвером DNS, который не предназначен для использования третьими лицами, убедитесь, что у него есть соответствующие элементы контроля доступа, ограничивающие круг пользователей этого резолвера. Дальше, пожалуйста.

Меры по снижению рисков для элементов управления конечными точками и сетями. Антивирус — это то, что существует уже давно и до сих пор актуально для многих пользователей. В отчете мы не стали тратить много времени на обсуждение антивирусов, но кратко упомянули о них. Строгий контроль над выбором резолвера DNS означает, что в наши дни множество устройств получают данные из сети, от DHCP-сервера, например. TCP-сервер сообщает, какой резолвер использовать. Обычно это работает, но есть также способы, позволяющие с помощью вредоносного ПО или других векторов атак изменить рекурсивный DNS-сервер, данные о котором были передан устройству, на что-то другое. Сетевые операторы должны обратить на это внимание. Либо блокируйте неавторизованные резолверы DNS на брандмауэре, либо выполняйте другие проверки, чтобы убедиться в том, что используемый устройством резолвер DNS является правильным и подходящим. Конечно, опять же, для организаций, которые способны защитить своих

пользователей, что-то вроде брандмауэра DNS является хорошей идеей, действительно позволяющей обеспечить, чтобы эти пользователи посещали в сети только подходящие и безопасные места. Дальше, пожалуйста.

Что касается мер по снижению рисков, рассмотренных нами в отчете, они были разделены на категории, которые я в основном уже рассмотрел. Некоторые из них — это, опять же, проблемы с учетными данными, средства контроля доступа к учетным записям пользователей и так далее. Гэвин рассказал о подмене ресурсов, а также об уязвимостях кода и протокола. В отчете рассматривается использование DNS в качестве вектора атаки, а не в качестве цели. Разумеется, рассматриваются атаки типа «отказ в обслуживании» и механизмы реагирования на инциденты. Думаю, это мой последний слайд. И теперь мы передаем слово Марку.

МАРК РОДЖЕРС: Здравствуйте! Мой микрофон не включается. Хорошо. Следующий слайд. Я расскажу о рекомендациях, которые были сформулированы в результате проведенных в группе обсуждений. Существует очевидная связь с рассмотренными векторами атак и мерами по снижению рисков. В целом они разделены на пять категорий: операционные улучшения, исследования, заключение контрактов, финансирование, а также обучение и ознакомление. Следующий слайд.

Первая рекомендация заключается в том, что ICANN следует в сотрудничестве с другими организациями, такими как SSAC, GNSO, ccNSO, TLD-OPS, составить программу теоретических учебных занятий. С помощью этой программы следует обеспечить возможность отработки выполнения оперативных функций при возникновении инцидентов для выявления возможных недостатков в оперативной деятельности. Занимаясь этим постоянно, ICANN и другие органы смогут выявлять, регистрировать и отслеживать эти операционные недостатки, чтобы затем над ними можно было поработать и указать на них в будущих рекомендациях. Следующий слайд.

Было дано несколько рекомендаций по проведению исследований. Первая касается злоупотреблений DNS. Картина угроз никогда не бывает статичной. Она постоянно меняется, как и злоупотребления DNS. Вчерашние методы злоупотреблений развиваются и завтра станут новыми. А также открываются новые возможности по мере внедрения различных технологий или развертывания различных архитектур DNS. Поэтому мы порекомендовали постоянно проводить исследования в области злоупотреблений DNS, чтобы обеспечить постоянное понимание текущей картины злоупотреблений и мест, где они происходят, работая на опережение.

Следующая рекомендация состоит в том, что следует исследовать улучшения безопасности DNS. Как и картина угроз, улучшения безопасности DNS постоянно меняются. Опять же, мы считаем,

что должна быть разработана программа исследования ограничений, рисков и преимуществ различных улучшений безопасности DNS. Некоторые из этих улучшений перечислены ниже в отчете. Но образ мыслей в целом, как и в случае злоупотреблений, следующий: нам нужно постоянно следить за этим, вести мониторинг и создать контур обратной связи, позволяющий постоянно выявлять недостатки и находить улучшения, а также постоянно получать обратную связь.

Если обратиться к разговорам об аутентификации в предыдущих разделах, мы считаем, что необходимо изучить соответствующие передовые методы аутентификации. Я думаю, что ICANN вместе с сообществами других соответствующих организаций должна провести исследование и предложить отчет о том, что следует считать наилучшей практикой аутентификации с учетом различных ролей и рисков в DNS. Следующий слайд.

Что касается контрактов и финансирования, рекомендация насчет контрактов предусматривает работу ICANN по предоставлению сторонам, связанным договорными обязательствами, полномочий внедрять улучшения безопасности в системы регистрации доменов и авторитативные службы имен, насколько это возможно. Мы считаем, что такие полномочия позволят организациям значительно повысить безопасность DNS.

Следующая рекомендация посвящена программам выплаты вознаграждений за обнаружение ошибок. Группа очень активно обсуждала этот вопрос, потому что есть много мнений насчет того, где можно использовать такие программы, насколько они эффективны и как их следует применять. Однако мы все согласились, что ICANN должна оценить осуществимость программ выплаты вознаграждений за обнаружение ошибок в DNS. Поскольку есть ряд областей, где, например, инфраструктура DNS не принадлежит конкретной организации или инфраструктура DNS больше не поддерживается, и было бы полезно иметь управляемую программу выплаты вознаграждений за обнаружение ошибок, чтобы уделить внимание таким областям, таким компонентам программного обеспечения для выявления уязвимостей. И поскольку это очень непростая тема, мы считаем, что лучший подход — выполнить оценку целесообразности, чтобы выбрать наилучший подход, найти наиболее экономичный подход и посмотреть, каким образом можно передавать информацию об уязвимостях в подходящие организации, чтобы гарантировать ее надлежащее рассмотрение. Следующий слайд.

Мы считаем, что существует острая потребность в обучении и ознакомлении. Мы считаем, что ICANN должна заняться созданием и распространением учебных программ, которые стимулируют внедрение заинтересованными сторонами DNS механизмов аутентификации, соответствующих стандартам, для

всех взаимодействий, требующих аутентификации. Следует информировать такие заинтересованные стороны не только потому, что они подвергаются риску в связи со слабыми схемами аутентификации, но и потому, что слишком много устаревших схем аутентификации используется просто по незнанию. И мы считаем, что обучение и ознакомление дает хорошие возможности для перехода к более надежным схемам аутентификации.

Блокировка на стороне регистратуры. ICANN следует предпринять усилия по совершенствованию документации, для лучшего понимания функций блокировки на стороне регистратуры и содействия их использованию в необходимых случаях, а также для лучшего понимания различий между блокировкой на стороне регистратуры и блокировкой на стороне регистратора. Владельцы доменов должны иметь возможность найти четкие определения того, что обеспечивают или не обеспечивают эти функции, и каковы различия между ними. ICANN также следует рассмотреть возможность поспособствовать стандартизации минимальных требований к службам блокировки на стороне регистратур и регистраторов. Следующий слайд.

Мы считаем, что необходимо повышать осведомленность о передовых методах обеспечения безопасности инфраструктуры. ICANN необходимо сотрудничать с такими инициативами, как MANRS и KINDNS, чтобы оценивать степень их принятия, составлять соответствующие отчеты и использовать эти отчеты

для подготовки целевых учебных материалов, повышающих осведомленность в вопросах безопасности инфраструктуры. ICANN следует воспользоваться передовым опытом, накопленным в рамках этих инициатив, и распространять информацию об этом опыте среди сторон, связанных договорными обязательствами, и сообщества ICANN. В тех случаях, когда передовых методов не существует, ICANN должна поощрять разработку и развертывание таких методов и способствовать внедрению функций улучшения безопасности DNS во всей экосистеме DNS. В качестве примеров можно привести DMARC, SPF, TLSA, DANE, DNSSEC и так далее.

Далее идут рекомендации, касающиеся блокировки и фильтрации DNS. ICANN следует создать информационные и учебные материалы, чтобы содействовать пониманию сообществом ICANN, сторонами, связанными договорными обязательствам, и другими заинтересованными сторонами рисков и преимуществ блокировки и фильтрации DNS по соображениям безопасности и стабильности во всем глобальном сообществе DNS. Следующий слайд.

Что касается реагирования на инциденты, ICANN должна вместе со всеми соответствующими сторонами стимулировать разработку и внедрение формализованного процесса реагирования на инциденты для всей отрасли DNS, позволяющего взаимодействовать с другими участниками экосистемы. Такая деятельность охватывала бы реагирование на инциденты, а также защищенный обмен информацией об угрозах

и инцидентах. И это опять же можно связать с теоретическими учебными занятиями, чтобы гарантировать, что любые такие планы реагирования на инциденты могут быть введены в действие, выявляя все операционные недостатки.

Рекомендация E6. Осведомленность о скрытых каналах. ICANN следует публиковать учебные материалы об использовании скрытых каналов в качестве вектора атаки, что может рассматриваться как злоупотребление самой DNS и, как таковое, требует решения других проблем, связанных со злоупотреблениями DNS. Следующий слайд.

Что касается двух первоочередных задач, которые мы могли бы выбрать из сформулированных рекомендаций, мы считаем, что первая — это рекомендация R3: изучить оптимальные передовые методы аутентификации. И вторая — это рекомендация E5: реагирование на инциденты. Следующий слайд.

Хорошо. Вам слово, Мерике.

МЕРИКЕ КЭО: Отлично. Большое спасибо. Все, кто хочет получить дополнительные сведения о технической группе и ознакомиться с ее уставом, документом с описанием круга вопросов, подлежащих изучению, планом и сроками работы, повестками дня и протоколами заседаний, а также с другими ресурсами, могут посетить сайт этой группы. И, как упомянул Джон, отчет

будет опубликован на следующей неделе вместе с заметкой в блоге. Я просто предупреждаю вас заранее, что в нем намного больше подробной информации, чем мы смогли представить здесь за такой короткий промежуток времени. Там много информации очень высокого качества, которую вы сочтете весьма полезной, как мне кажется. Разумеется, я надеюсь, что генеральный директор ICANN сочтет этот отчет полезным, и будут приняты соответствующие меры. А сейчас я хотела бы открыть раздел ответов на любые оставшиеся вопросы. На данный момент я не вижу никаких вопросов в модуле.

ВЕНДИ ПРОФИТ: По-моему, на все вопросы в модуле были даны письменные ответы.

МЕРИКЕ КЭО: Да. Мне интересно, есть ли новые вопросы. Напишите их, воспользовавшись функцией вебинара Q&A, и мы с радостью на них ответим. Хорошо. Снова возник вопрос: «Где я могу получить итоговый отчет?» Итоговый отчет будет опубликован на следующей неделе параллельно со статьей в блоге. Я полагаю, что соответствующая ссылка также появится на вики-сайте, на который я только что указала. Был задан вопрос: «Прилагаются ли эти вопросы и ответы к записи?» Я оставлю это на усмотрение персонала. Будет ли стенограмма опубликована вместе с записью?

ВЕНДИ ПРОФИТ: Позвольте мне уточнить это у команды MTS.

МЕРИКЕ КЭО: Хорошо. Большое спасибо. Спасибо за вопрос, Донна. Как вы понимаете, я хочу сказать, что за последние 18 месяцев на эту работу было потрачено очень много времени, и на самом деле профессиональная компетентность этой группы специалистов различных направлений не вызывает никаких сомнений. Она работала превосходно. Я хочу поблагодарить всех без исключения участников, которые внесли свой вклад в составление этого отчета.

На данный момент я не вижу других вопросов. Если это так, то я хочу поблагодарить всех участников этого подготовительного заседания. Еще раз попрошу вас ознакомиться с отчетом, когда он будет доступен на следующей неделе, и с нетерпением жду того, что с ним произойдет.

ВЕНДИ ПРОФИТ: У нас в модуле есть еще один вопрос, на который нужно ответить: «Каковы основные мотивы злоумышленников? Из каких они стран?»

МЕРИКЕ КЭО: Я отвечу на этот вопрос. Но любой другой член TSG также может внести свой вклад. Мотивы самые разные. Это могут быть просто отдельные лица, есть также организованная преступность, а источник угрозы на самом деле может находиться в любой стране. Такова природа виртуального мира, в котором мы сегодня живем. Ладно, на этом я закрою заседание. Всем большое спасибо за участие.

[КОНЕЦ СТЕНОГРАММЫ]