САН-ХУАН — Принципы работы: Понимание проблем злоупотребления DNS
Понедельник, 12 марта 2018 г. - 13:30 – 15:00 по AST
ICANN61 | Сан-Хуан, Пуэрто-Рико

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Добрый день. ICANN61. 12 марта. Принципы работы: Понимание проблем злоупотребления DNS.

КАТИ ПЕТЕРСЕН (CATHY PETERSEN): Добрый день! Мы скоро начнем очередную сессию по принципам работы, «Понимание проблем злоупотребления DNS», через пару минут. Спасибо.

Еще раз добрый день всем присутствующим. Добро пожаловать на сессию по принципам работы, посвященную проблемам злоупотребления DNS. На этой сессии докладчиком будет Карлос Алварез из офиса технического директора. Карлос?

КАРЛОС АЛВАРЕЗ (CARLOS ALVAREZ): Большое спасибо, Кати. Спасибо всем присутствующим в этом зале. Также я вижу достаточно участников онлайн. По-моему, их вроде бы 23, может быть, станет больше по ходу сессии.

Нам предстоит обсудить очень важную тему. Очень актуальную. Некоторые ее моменты весьма спорные, и мы все должны уделить ей должное внимание. Мы будем говорить о злоупотреблении DNS.

Сначала мы обозначим некоторые аспекты обсуждения. Аспектов несколько. Злоупотребление DNS можно рассматривать с нескольких точек зрения. Сегодня мы обозначим некоторые из них, а потом обсудим примеры злоупотребления или неправильного использования DNA. Мы поговорим об эволюции интернет-среды и о том, как она связана с DNS. И в конце мы вкратце рассмотрим злоупотребление DNS в контексте ICANN.

Первый момент, о котором стоит упомянуть, — у понятия «злоупотребление DNS» нет единого глобально принятого определения. На слайде, который вы видите, говорится, что есть [варианты] определений, которые включают в себя такие подтемы, как киберпреступность, хакерство и злонамеренное поведение.

Можно решить, что злоупотребление DNS попадает в одну их трех категорий. Это может быть повреждение данных, отказы в обслуживании и угроза конфиденциальности. Разумеется, неправильное использование DNS отличается от злоупотребления DNS. Я вкратце читаю то, что написано на слайде.

Неправильное использование означает умышленное введение в заблуждение, попустительство или нежелательную деятельность с активным использованием DNS или процедур удаления доменных имен или преобразования. Давайте посмотрим, что это означает. Мы увидим это позже.

Что говорили в GAC в попытке найти определение или предоставить средства для понимания смысла злоупотребления DNS? Что говорили в GAC по поводу такой обширной темы? В своем коммюнике GAC указал механизмы защиты, применимые ко всем новым gTLD, в выдержке из документа, который был посвящен сокращению случаев неправильного использования. В нем упоминались определенные типы злоупотреблений, как то: распространение вредоносного программного обеспечения, эксплуатацию ботнетов, фишинг, пиратство, нарушение прав на товарные знаки и авторских прав, мошенничество, незаконное копирование или иное участие в деятельности, противоречащей применимому законодательству.

Это определение выглядит довольно широким, и кое-кто придерживается мнения, что некоторые из указанных разновидностей не обязательно являются техническим злоупотреблением DNS как технической системы. Но, как я сказал, сейчас мы рассказываем о точках зрения,

которые есть у сообщества. Это одна из них. Есть и другая точка зрения, не рассматривающая нарушение авторских прав и прав на товарные знаки, а также, в определенных случаях, мошеннические или вводящие в заблуждение действия в технической DNS как таковой, по множеству причин.

Большой вопрос — на этой сессии я оставлю его без ответа — состоит в том, стоит ли рассматривать спам как злоупотребление DNS, системой доменных имен.

Со стороны сообщества, занимающегося операциями и безопасностью, а также правоохранительных органов, спам рассматривается как индикатор и предшественник других типов злонамеренной деятельности. Сам по себе, по крайней мере до сегодняшнего дня, он не считался как таковым техническим злоупотреблением DNS, глобальной системы доменных имен.

Занимаясь изучением угроз и анализом данных и обнаружив, что недавно началась очередная спам-кампания, вы можете определить криминальную инфраструктуру, которую проблемные игроки используют для проведения этой кампании. Если продолжать следить за их деятельностью, рано или поздно вы...обычно рано, а не поздно...увидите последующие действия, которые будут именно следовать за рассылкой спама. Это может

быть распространение вредоносного ПО. Это может быть распространение материалов, связанных с жестоким обращением с детьми. Это может быть фишинг...разные вещи. Проще говоря, злоупотребление DNS означает все, что нацелено на атаки или злоупотребление инфраструктурой DNS. Это будет показано на слайдах, которые я приготовил.

Существует множество способов рассматривать злоупотребление DNS. Мы обсудим два способа раскрытия этой темы. Первый — с точки зрения злоупотребления преобразованием доменных имен, технической стороной того, как доменные имена преобразуются в IP-адреса. Вторая точка зрения, о которой мы будем говорить, связана с регистрацией доменных имен, испытанием регистрационных услуг.

Преступники могут по-разному злоупотреблять этими услугами, предоставляемые регистраторами и регистратурами. Мы будем об этом говорить.

Неправильное использование DNS относится к злонамеренному использованию протокола DNS на более техническом уровне или процессов регистрации. Мы рассмотрим примеры всех этих разновидностей более подробно, если все будет работать. [Я хочу показать] – да. Вот сюда.

Извините. Не нужно читать все эти слайды. Смысл не в этом. Смысл в том, чтобы показать вам операционные элементы DNS в упрощенном виде.

Вот тут, над словом синего цвета, указаны авторитативные серверы имен, на которых хранятся авторитативные данные для каждого доменного имени или для каждого TLD. Сразу под ними находятся рекурсивные резолверы имен, которые выглядят как серверы DNS, которые ваш ISP — компания, предоставляющая вам доступ в интернет, — позволяет вам использовать. Они предоставляют вам услуги по разрешению DNS.

Затем идет клиент или резолверы. Что такое резолвер? Вот здесь он показан. Это функция моего браузера, к примеру, которая обеспечивает поиск информации для использования тех ресурсов, которые я хочу использовать.

Например, если я открою браузер и введу www.ICANN.org, то будет активирована функция резолвера, которая преобразует доменное имя в IP-адрес, на котором хранится содержимое для www.ICANN.org. Она загрузит его на мое устройство, и я смогу его видеть и взаимодействовать с ним, например.

Эти три операционных элемента DNS становятся мишенью атак. Мы увидим, что, по сути, мишенью атак становится все, что находится онлайн.

Примеры, вот где начинается самое интересное. Давайте сосредоточимся на отражении/усилении, которые лежат в основе DDoS-атак (типа «отказ в обслуживании»).

Что такое отражение? Отражение означает, что вы можете отправить пакет и фальсифицировать информацию об IP-адресе источника, заставив сервер думать, что ее отправили откуда-то еще, и отправить ответ уже на этот другой IP-адрес. То есть, если я хочу атаковать Кати, я отправляю пакет на DNS-сервер и IP-адрес, который я прикрепляю к пакету, будет показывать, что пакет пришел от Кати, а не от меня.

Если я это делаю при помощи так называемых открытых резолверов, то есть DNS-серверов, которых существуют тысячи и тысячи, которые не фильтруют IP-адреса, от которых поступают запросы, и отвечают на запросы, поступающие из любого региона мира, то Кати подвергнется лавинной рассылке, так как я разошлю DNS-запросы на все эти тысячи и тысячи открытых резолверов, за которыми никто не наблюдает. Все они будут думать, что все запросы отправляла Кати, поэтому отвечать они будут именно ей. Вот что такое отражение.

Другой вариант — усиление. Что означает усиление? Это означает, что вы берете эти запросы, которые я отправляю, — они крохотные. Обычно это всего одна строка команды. Эта строка может быть просто DIG DNS-сервер доменное имя ANY. Оп! Вот и все. Это 7 байтов, наверное. Реально очень мало. Это всего лишь строка текста, а вот ответ будет огромным. Его размер может быть 2,3, 2,5 или 2,7 мегабайт. Умножьте это на тысячи запросов, которые рассылают мои ботнеты. Помните ботнеты, эти обширные сети зараженных устройств, которыми управляют преступники? В них может быть сотни тысяч зараженных устройств. Преступник, управляющий ботнетом, может заставить все эти зараженные устройства отправлять запросы на все открытые резолверы, которые будут отправлять ответы Кати.

То есть тут эффект приумножается благодаря числу зараженных устройств, которыми я управляю и которые входят в мой ботнет, а также тысячам открытых резолверов, которые я использую, и способу отправки команды — при помощи DIG-запроса. DIG — это команда, позволяющая получать информацию от DNS. Она запускает отправку ответа. И они так составляют эту команду, что ответ просто огромный, как я уже говорил.

Так что Кати, вероятнее всего, окажется оффлайн, если она не использует службу защиты от DDoS или вроде того. Если она не способна справиться с трафиком, который к ней поступит, она окажется оффлайн. Это невозможно предотвратить.

Первая крупная DDoS-атака, которая [неразборчиво] с использованием DNS как вектора атаки, произошла в 2003 г. и была направлена против Spamhaus. Организация Spamhaus работает не только со спамом, но и с вредоносным ПО и прочим. Они проводят расследования. Они предоставляют интересные сведения, позволяющие бороться с угрозами и предотвращать их.

И, конечно, методы атак становятся все более продуманными. Ну, разумеется, DNS — это не единственный вектор атак, естественно. Это лишь один из множества, но как протоколом ей злоупотребляют и очень часто.

Мы еще поговорим об отравлении кэша или атаках на истощение ресурсов. Это предпоследняя тема. Последнюю атаку DNS, атаку посредника, мы также обсудим через пару слайдов.

Собственно, вот о чем я сейчас и говорил. Это крупная DDoS-атака, использующая отражение, отправку пакетов

с фальшивыми IP-адресами источника, заставляющими все эти открытые резолверы думать, что запросы рассылает устройство Кати. И запрос, который они получили, составлен так, что влечет за собой огромный ответ. Это вектор усиления. Кати подвергается лавинной рассылке. Именно про это я сейчас и говорил.

Это был не я. Я, похоже, опережаю сам себя. Я переборщил с кофе. На чем мы остановились?

Вот. Еще один способ атаки DNS — это нарушение работы чьих-нибудь DNS-серверов. DNS-сервер — это часть инфраструктуры, обеспечивающей разрешение доменного имени. То есть, если я стираю ваше имя «карлос.что-то там», мне придется настроить, в идеале, как минимум два сервера, от которых DNS, как глобальная система, должна получать информацию о ресурсах, которые я ранее привязывал к этому имени. Другими словами, я скомпоную и сделаю эту информацию доступной для этих DNS-серверов — IP-адреса; проще говоря, где будет расположен мой почтовый сервер, где будет находиться мой веб-сервер, где будет находиться мой FTP-сервер и так далее.

И если кто-то отключает мои DNS-сервера от сети, никто не сможет получить эту информацию, то есть я не смогу ни получать, ни отправлять электронную почту. Люди не

смогут получить доступ к моему сайту и так далее. То есть могут быть существенные последствия, если речь о значимом доменном имени. Я не говорю, что «карлос.что-то там» — это значимая мишень. Его, наверное, и не существует, но все возможно.

Этот метод...атака такого типа...предполагает, что преступники злоупотребляют протоколом TCP. Когда вы отправляете TCP-пакет на сервер, от сервера приходит ответ. Это, опять же, если говорить максимально просто. Когда сервер отвечает на TCP-подключение, и устройство, инициировавшее подключение, и отвечающий на это сервер проводят квитирование, при котором образуется канал связи, поддерживаемый обоими устройствами. Это означает, что оба устройства должны выделить определенные ресурсы для поддержания этого канала связи.

И если в ботнете у вас много зараженных устройств, и все они отправят запросы/ответы на DNS-сервер так, чтобы этому серверу пришлось выполнить слишком много TCP-квитирований и выделить ресурсы на поддержание всех этих установленных каналов связи по TCP, то вскоре наступит такой момент, когда у сервера не останется доступных ресурсов для назначения дополнительных TCP-соединений и, соответственно, никто больше не сможет получить от этого сервера информацию о DNS.

Он останется онлайн, но вообще не сможет отвечать на запросы. Как сказано на слайде, разрешение имен происходит некорректно или прервано.

Если повезет, вы сможете получить ответ через пару минут. Умножьте это на тысячу, если речь о доменном имени с большим трафиком, или вы потеряли возможность разрешения. Это худший сценарий, которого нужно избежать всеми силами.

Отравление кэша. Это аферизм. Вот как плохие парни проявляют креативность, ну, как обычно...в смысле, бывает и так. Иногда они такое выкидывают. Помните, на предыдущем слайде мы говорили, что в самом верху у нас авторитативные DNS-серверы, как если бы я создал и зарегистрировал «карлос.что-то там» и привязал к нему «ns1.карлос.что-то там» и «ns2.карлос.что-то там», чтобы предоставить DNS информацию, связанную с моим почтовым сервером и веб-сервером? Это мои авторитативные DNS-серверы.

У каждого ISP – там много народу; 9.9.9.9 или 8.8.8.8 или OpenDNS или UltraDNS; DNS предоставляет очень много – в рекурсивном формате, что означает, что они задают вопросы от лица кого-то другого. Есть некоторые рекурсивные резолверы, как их называют, которые не очень хорошо защищены. Они уязвимы. Только

представьте все эти тысячи интернет-провайдеров во всех регионах, которыми могут управлять маленькие компании со скудными ресурсами. И вот у них есть инфраструктура для работы, но нет ресурсов для ее защиты.

Когда эти серверы защищены недостаточно хорошо, преступники могут компрометировать их множеством способов, один из них, допустим, если я пользователь интернет-провайдера, рекурсивный резолвер которого скомпрометирован, и я отправляю запрос на данные, связанные с, к примеру, PayPal.com, я могу получить корректный ответ, но также, из-за того, что сервер скомпрометирован, преступники добавят к нему дополнительный кусок информации. Этот кусок будет, например, такой: «И, кстати, вот IP-адрес BankOfAmerica.com».

И это приведет к автоматическому обновлению временной памяти моего устройства, его кэш-памяти. Я бы сказал, это должен быть файл хоста. Когда это происходит, как вы думаете, куда перейдет мое устройство, когда я в следующий раз захочу зайти на BankOfAmerica.com? Если это случится в течение определенного периода, то оно перейдет на IP-адрес, который мне подсунули преступники. Это плохой сценарий. Ничего хорошего.

Что произойдет тогда? Я перейду на сервер, которым управляет преступник. Я увижу то содержимое, которое он хочет, чтобы я видел, в данном случае это будет фишинговый сайт, копирующий Банк Америки. И я с радостью предоставлю им свои учетные данные, а это будет совсем не хорошо для моих личных финансов, понятное дело.

Преступники могут делать что-то подобное и другими способами. Они могут напрямую компрометировать ваше устройство и изменять вашу DNS-конфигурацию. Позже мы рассмотрим пример вредоносного ботнета, который, по моему, уничтожили четыре года назад. Если мое устройство настроено для рассылки DNS-запросов на, к примеру, 1.1.1.1, они меняют этот IP-адрес здесь или на ноутбуке, и вместо этого корректного IP-адреса, необходимого пользователю, они указывают свой собственный. Они указывают IP-адрес DNS-сервера, которым управляют и который настроен для предоставления IP-адресов в их собственную инфраструктуру. Другими словами, все пользователи с скомпрометированными устройствами будут переходить на их собственные веб-сайты, что, опять же, совсем не хорошо. Очень скоро мы это обсудим.

В подобной ситуации, если говорить именно об отравлении кэша таким методом, они заставляют

скомпрометированное устройство пользователя отправлять запросы на их DNS-сервер. Допустим, я запрашиваю сайт, не относящийся к преступникам — новый сайт (хотя к ним все что угодно может относиться). Допустим, «новости.что-то там» — это сайт, не относящийся к преступникам. Точно так же, как они делали в предыдущем примере, о котором я сказал, они прибавляют дополнительный кусок информации к ответу, который их сервер отправляет на мое устройство. Этот дополнительный кусок будет также IP-адресом: «И, кстати, вот IP-адрес веб-сайта вашего банка». И опять же, пока не прошло определенное время, я могу отправить запрос на доменное имя своего банка, так как хочу зайти в систему онлайн-банкинга, и вуаля! Я оказываюсь на веб-сайте преступника. Снова ничего хорошего для моих финансов.

DNSChanger — это как раз такой тип вредоносного ПО, о котором я говорил. Именно это он и делал. Он изменял DNS-конфигурацию, необходимую пользователю. Он может проникать практически везде. Преступники, которые управляли этим ботнетом — умы, стоявшие за этой операцией,— смогли очень хорошо нажиться. К тому времени, когда правоохранительные органы проводили свою операцию, им удалось предоставить неоспоримые доказательства, что преступным путем было получено 25

миллионов евро. Это не означает, что они не заработали даже больше. Это лишь значит, что это та сумма, которую правоохранительным органам удалось подтвердить доказательствами.

С помощью DNSChanger преступники изменяют DNS-конфигурацию на пользовательских устройствах. То, что они делали, выглядело вполне невинно — они заменяли рекламу, которую пользователи видели при посещении веб-сайтов. Если я с утра на работе открывал свой любимый сайт новостей, пока попивал кофе, то вместо реальных объявлений я бы видел те, которые разместили преступники. Им это приносило постоянный доход. Это происходило очень долго. Это золотая жила.

Никакого вреда она не приносит, на первый взгляд. Пользователи не замечали никакого подозрительного поведения своих устройств. Они по-прежнему могли получать доступ к нужному им контенту. Они по-прежнему могли работать в интернете и взаимодействовать с нужными ресурсами. То есть, понятно, ничего странного не происходило.

Но на самом-то деле происходило. Поэтому были приняты меры, и обеспокоенность была связана с тем, насколько много устройств было заражено. Я не помню точное количество устройств, но в этом ботнете были

сотни тысяч устройств, скомпрометированных этим вредоносным ПО в нескольких странах. Не хочу соврать, но стран было вроде бы около 20. Я полностью не уверен.

Но вопросы возникли, когда они...говоря «они», я имею ввиду правоохранительные органы...когда они захотели что-то сделать с этими DNS-серверами, которыми управляли преступники. Они могли их либо отключить, и в этом случае...как вы думаете, что бы произошло, отключи они все эти DNS-серверы? Учитывая, что все устройства пользователей отправляли DNS-запросы на эти серверы, что бы произошло?

Пользователи решили бы, что связь с интернетом прервалась. Они бы по-прежнему остались подключены к интернету, но их устройства не могли бы преобразовать ни одно имя, так как DNS-серверы бы не работали. То есть просто так их отключить они не могли.

Используя инжиниринг...назовем это так...они смогли заменить эти серверы на другие. Суд назначил для этих серверов администратора на определенное время, используя [национальные] группы CERT и другие методики. Во всех этих странах прошли информационные кампании, побуждающие пользователей очистить свои устройства.

Конечно же, с тех пор преступники не перестали совершать преступления. Они нашли множество других путей злоупотребления протоколом DNS и различными операционными элементами DNS, и некоторые весьма интересные, по крайней мере, с научной точки зрения, так как в них заметен творческий подход, с преступными целями, но творческий, например, скрытый канал просачивания данных. По-моему, про него на следующем слайде...нет. Давайте о нем поговорим.

Конечно, когда вы можете отправлять данные из скомпрометированной сети так, чтобы при этом администратор этой сети не знал, что их данные воруют, то это скрытое просачивание. DNS считается интересным скрытым каналом просачивания данных, так как обычно этот маленький порт, используемый для обмена данными в DNS, не заблокирован. Его нельзя заблокировать.

Трафик в сети передается через порты, из одного на другой. Протокол DNS использует порт 53. Хотя инженеры всегда могут найти способ переназначить порт во внутреннем порядке в собственной сети, тут могут быть свои осложнения. Поэтому его обычно не переназначают и не заменяют на другой порт. Это значит, что трафик через порт 53 нельзя заблокировать. Его очень трудно переназначить, поэтому его просто нельзя заблокировать. Если он заблокирован, то люди не смогут

использовать разрешение DNS, то есть они думают, что они оффлайн.

Что вообще происходит, когда возникает скрытый канал просачивания данных? Бывает по-разному — сейчас я могу вспомнить как минимум два варианта. Первый: вы компрометируете устройство, и оно начинает потихоньку отправлять DNS-запросы на DNS-сервер преступника. Дело в том, что в каждом DNS-запросе преступники заменили наименее релевантные биты на биты, соответствующие данным, которые они извлекают. Если группа инженеров или администратор сети будут изучать эти запросы, изучать трафик, они просто скажут, что это DNS-запросы. Им пришлось бы собрать все DNS-запросы, используемые для просачивания конкретного блока данных. По сути, понадобится анализ. Понять, что наименее релевантные биты были изменены, сложить воедино все эти наименее релевантные биты, попытаться из них что-то скомпоновать и в итоге понять, какую именно информацию хотели извлечь. Это первый вариант.

Другой вариант использования преступниками DNS для извлечения информации немного проще и предполагает использование записей TXT. Когда вы создаете доменное имя, вы по умолчанию будете администрировать или управлять так называемым файлом зоны.

В файле зоны вашего доменного имени вы определяет ресурсы, которые с ним связаны. Именно тут вы указываете информацию о своем сайте, почтовом сервере, FTP-сервере. Если у вашего домена есть подпись DNSSEC, то эта информация также туда попадет. Если вы располагаете всеми механизмами защиты ваших клиентов или в целом общественности...не знаю, может быть, кто-то из вас уже слышал о таких. Они по большей мере обозначаются аббревиатурами — SPF, DKIM и DMARC — и просто защищают пользователей, говоря простыми словами.

Информация всех этих типов помещается в так называемые TXT-записи. По большому счету, вы можете включить в TXT-запись все что угодно. Нет никаких ограничений на текст, который можно включить в TXT-запись. Это просто текст. Преступники используют и эти TXT-записи для извлечения информации. Они могут отправлять DIG-запросы с информацией, касающейся TXT-записей, на DNS-сервер, который в свою очередь собирает информацию, группирует ее и восстанавливает извлеченные данные, ну и так далее.

Fast Flux. По-моему, о ней будет сказано дальше. Если нет, то мы к ней вернемся, но думаю, о ней еще пойдет речь.

Регистрация доменных имен — это очень аппетитная мишень для атак. Это довольно очевидно. Преступники и злоумышленники, к сожалению, нарушают права законных провайдеров услуг регистрации доменов в пространствах gTLD и ccTLD. Они с удовольствием нарушают права регистраторов и реселлеров. Они с удовольствием присваивают большие количества доменных имен. Это очень проблематичная тема. Низкие цены на доменные имена привлекают злоумышленников, мне кажется, это вообще свойственно человеку. Дешевле значит лучше, так что они просто идут и регистрируют еще доменные имена, также, как и законные владельцы доменов и пользователи, которых привлекает возможность регистрировать имена, которые дешевле. Опять же, как я сказал, это свойственно людям. В этом нет ничего плохого. Такова жизнь.

Автоматическая регистрация доменных имен создает...и опять же, это не хорошо и не плохо. Просто такова природа этой отрасли. Она позволяет управлять крупными портфелями законных доменных имен, конечно же.

Но, к сожалению, без преступного злоупотребления тут тоже не могло обойтись. Когда я говорю об этом, я имею ввиду DGA-домены, по сути представляющие собой автоматический механизм создания и регистрации

большого числа доменных имен, которым пользуются преступники.

Что такое DGA? Это алгоритм создания доменных имен. Представьте себе ботнет. В каждом ботнете должна быть инфраструктура управляющего сервера, позволяющая преступникам отправлять точные команды и контролировать свою вредоносную инфраструктуру.

Что же происходит, если инфраструктуру уничтожить? В таком случае появится план B, C, D, E, F, G и так далее. Вот для чего нужны DGA. Когда ботнет понимает, что один из таких серверов, связанных с управляющей инфраструктурой, отключен, приостановил работу, не был определен и так далее, — раз! — и выполняется регистрация. Это просто пример. Есть способы работы DGA на любой вкус и цвет. Это просто упрощенное объяснение. Раз! И он [регистрирует] любую строку в любом TLD, и все начинается вновь.

Если возможность управления ботнетом потеряна из-за мероприятий по ликвидации угрозы, то можно зарегистрировать такую новую строку DGA? Раз! И все сначала. Они потеряли возможность управления ботнетом и просто продолжают работать.

Мы вскоре рассмотрим очень интересный случай. Надеюсь, мы скоро доберемся до этого слайда. Почему

атакующие и преступники регистрируют доменные имена для всего? Все, что вы только можете себе представить — по поводу фишинга, программ-вымогателей, распространения вредоносного ПО, мошенничества, поддельных товаров, нелегальных фармацевтических средств — всего чего угодно, они регистрируют имена.

Последняя строка...не знаю, почему она так отобразилась...это управляющий сервер ботнета, и это относится к стабильности и отказоустойчивости. Этот аспект вызывает наибольшее беспокойство в связи с масштабами атак.

Иногда возникают вопросы о нелегальных фармацевтических средствах — стоит ли считать это злоупотреблением DNS, когда очевидно, что это не связано со злоупотреблением DNS, по крайней мере, с технической точки зрения. Это больше похоже на подделывание — сайты, где это продается, и так далее. Это правда, но иногда под поверхностью скрыты гораздо более серьезные вещи. Я не могу вдаваться в подробности, но просто помните, что не все находится на поверхности. Вы можете видеть всего лишь несколько сайтов, где пытаются продать нелегальные, в некоторых странах, медикаменты. Но от всего этого страдает множество людей.

У вас есть вопрос? Прошу вас, подойдите к микрофону.

КАТИ ПЕТЕРСЕН: Вы можете использовать любые микрофоны на столах. Просим назвать свое имя, и кого вы представляете, если это актуально. Спасибо.

ФАРЗАНЕ БАДИЙ (FARZANEH BADII): Меня зовут Фарзане Бадий. Я председатель группы некоммерческих заинтересованных сторон. Я хочу задать вопрос от собственного имени. Говоря, что за доменным именем, с которого продаются нелегальные лекарства, могут стоять другие нехорошие вещи, вы имеете в виду, что может быть некое техническое злоупотребление? Или мы говорим о содержимом сайта?

КАРЛОС АЛВАРЕЗ: Я говорю о преступных операциях, для выполнения которых используются доменные имена. Это использование доменных имен, связанное с содержимым сайтов, и другая преступная деятельность, которая за этим следует.

ФАРЗАНЕ БАДИЙ: Просто небольшое замечание. То есть это не имеет никакого отношения к DNS и к техническому аспекту ее работы?

КАРЛОС АЛВАРЕЗ: С этой целью они используют доменное имя.

ФАРЗАНЕ БАДИЙ: Спасибо.

КАРЛОС АЛВАРЕЗ: Конечно.

Зачем платить, если можно взломать? Зачем вдруг преступники будут платить за доменные имена или кто-нибудь решит платить за доменные имена, если их можно взломать и просто захватить контроль над ними?

Бывают разные ситуации, в которых преступники вместо того, чтобы регистрироваться, предпочтут отключить и незаконно захватить доменные имена. Как они это делают? Они могут компрометировать учетные данные пользователя. Они могут компрометировать учетные данные владельца домена, с помощью которых он получает доступ к панели управления. Панель управления — это веб-интерфейс, позволяющий владельцам доменов управлять доменными именами.

Представьте, что преступная организация хочет захватить определенное значимое доменное имя или хочет навредить клиентам определенного банка. Они могут просто запустить обычную фишинговую рассылку, целенаправленную фишинговую кампанию, нацеленную на сотрудников этого банка, после определенного социального инжиниринга, как обычно, хитростью заставить работников банка нажать на ссылку, на которую нажимать не стоило бы, а потом украсть учетные данные.

Все, что случится после этого, целиком зависит от преступника. Они могут просто создать домен третьего уровня под доменом второго уровня, который вы видите. Если бы мой банк оказался в такой ситуации, допустим, мой банк «карлосбанк.что-то там», то преступник может создать домен «фишинг.карлосбанк.что-то там» и рассылать электронную почту в рамках фишинговой кампании, более эффективно убеждая жертв, ведь они будут видеть, что домен второго уровня — это действительно реальное доменное имя моего банка.

Или они могут целиком заменить DNS-серверы. Они могут изменить любую информацию, которая связана с доменным именем. Они могут изменить любую запись. Они могут удалить целый набор данных из файла зоны для этого имени.

И опять же, были ситуации, когда это, к сожалению, происходило, и регистраторы с недостаточно защищенной инфраструктурой были скомпрометированы. Это случается очень редко, что хорошо, но такие случаи были. Когда подобное случается, это совершенно не радостно. К счастью, в этих крайне немногочисленных случаях преступники атаковали конкретные значимые цели, и регистраторы реагировали очень быстро. Вообще, с тех пор уже прошло какое-то время. На эту ситуацию тогда отреагировали очень четко. Преступники намеревались захватить такие цели, захват которых был гарантирован при условии получения контроля над этими серверами.

Так что со стороны пользователей вы видите, что, если владельцев доменов хитростью убедят нажать на ссылку, потом пройдет обычный фишинг, который будет успешным. Или же атака на инфраструктуру регистрации, если она окажется успешной.

Ну, это еще одна сторона фишинга. У скольких владельцев доменов могут быть одинаковые учетные данные для доступа к панели управления, через которую они управляют доменными именами? У скольких владельцев доменов могут быть те же самые учетные данные для доступа к панели управления, что и учетные данные, которые ранее были скомпрометированы? Этого

нельзя сказать, если речь о десятках нарушений и крупных взломов, которые происходят каждую неделю, по сути, или каждый месяц.

Подстановка учетных данных позволяет преступникам совершать попытки входа в максимально возможное количество служб, используя пары имен пользователей и паролей, скомпрометированных в ходе предыдущей кражи данных. Когда им это удается, они проникают в систему и все, вам конец. И тут ничего нельзя предугадать. Это невозможно проверить. Совершенно нельзя предугадать, сколько владельцев доменов повторно используют свой пароль для управления регистрациями домена? Как обычно, здесь нужно понимание, исключительно понимание.

Fast flux: вот она. Fast flux — это технология, с помощью которой преступники очень быстро перепрыгивают с одного IP-адреса на другой, чтобы все больше запутывать работу правоохранительных органов и специалистов по предотвращению угроз безопасности.

Для этого в своих файлах зоны они устанавливают короткие TTL. TTL — это время существования. Это время, в течение которого действителен IP-адрес, который, например, может быть привязан к сайту. По истечении этого времени рекурсивные резолверы на

стороне понимают, что снова должны отправить запрос, чтобы еще раз получить эту информацию. Когда они это делают, им сообщается другой IP-адрес. Так что, видя короткие TTL, например 120 секунд, 180 секунд, 2, или 3, или 4 минуты, исследователи сразу же думают:«Так-так-так».

Но здесь есть оговорка: дело в том, что крупные CDN... CDN — это сети передачи данных...в своей работе также используют короткое TTL для обеспечения стабильности, распределения нагрузки и по другим причинам технического характера. Но это другой вопрос. Так что, если вы исследуете угрозы, вы понимаете, какие крупные сети используют TTL, и все в порядке. Но если вам попадается новый домен с коротким TTL, привязанным к нему, и с какой-то [ранее не встречавшейся] инфраструктурой, которую можно было видеть у спамеров, например, то это сразу же вызывает подозрения. Вот когда рука исследователя угроз сразу же тянется в целях безопасности заблокировать трафик, связанный с этой инфраструктурой.

Что происходит, если вы работаете в правоохранительных органах и ведете расследование против преступной инфраструктуры/деятельности, связанных с применением Fast Flux, если вы видите, что содержимое находится на этом сервере в этой стране, а

через две минуты там уже нет этого содержимого, но оно появляется на другом сервере в другой стране, а еще через две минуты содержимое перепрыгивает на другой сервер в третьей стране, а еще через две минуты — на следующий сервер в четвертой стране или пятой стране и так далее? Как тогда поступают правоохранительные органы?

Все сложно. Очень сложно. Fast Flux с удвоенной скоростью — вот что это такое. Эту технологию мы видели в крупномасштабном...как бы это назвать? ...облачном сервисе преступников. Он называется Avalanche. В Avalanche злоумышленники использовали технологию Fast Flux с удвоенной скоростью. Это означало, что они очень часто сменяли DNS-серверы.

Если я бы хотел отправить запрос на «карлос.что-то там» прямо сейчас, я бы отправил запрос на «ns1.карлос.что-то там». Если бы я отправил запрос через две минуты я бы отправил запрос на «ns1.кати.next». Еще через две минуты я бы отправил запрос на «ns3.камерон.yoohoo». Каждые две-три минуты DNS-серверы бы менялись. И тогда DNS-серверы были бы наверху этого всего, меняя IP-адреса каждые две или три минуты, или короткое TTL, которое установили преступники. Так что это было в два раза хуже и в два раза противнее, а еще в два раза запутаннее, но профессионалы смогли это понять и

решить эту проблему. Плохие парни попали за решетку. И главарь попал за решетку.

Я говорил, что DNS — это скрытый канал просачивания данных, и что типы вредоносного ПО, по сути...это нацелено не только на извлечение данных, но и, в большей мере, на получение реального контроля над вредоносным ПО, заражающим или компрометирующим устройства. Посредством DNS преступники отправляют команды на устройства. Преступники изменяют вредоносное ПО, скомпрометировавшее устройства. Преступники могут внедрять новое вредоносное ПО через DNS.

Это такая головная боль, ведь, как я сказал, порт 53, предназначенный для обмена данными с DNS, нельзя заблокировать. То есть только от администратора сети зависит, насколько эффективные методы будут использоваться для обнаружения подобных вещей.

Есть определенные методы, о которых я сейчас не могу рассказать, потому что на это уйдет еще три часа. Это зависит от них. Внедрение этих методов зависит от администратора каждой сети.

Мы только что это увидели. Два примера вредоносного ПО, которое этим занимается, как и многие, многие другие типы программ, — это Feederbot и Morto. Здесь вы видите,

что управляющий сервер ботнета шифрует инструкции в TXT-ответах DNS. И скомпрометированное устройство отправляет запрос на DNS-сервер, причем злоумышленник настроил этот DNS-сервер таким образом, чтобы тот отправлял ответ в форме...запрос был на TXT-запись, и в этой TXT-записи содержатся инструкции для скомпрометированного устройства, говоря в общих чертах. Это могут быть абсолютно любые инструкции. В них может быть сказано:«Атаковать эти цели и этот трафик таким-то способом». Это может быть что угодно.

Среда DNS эволюционирует. Атака DDoS какой-либо службы. Поговорим о Mirai. Кто-нибудь помнит Mirai? Да. Тогда сложилась сложная ситуация.

Mirai был...как бы лучше его назвать? Между поставщиками так называемых услуг бутеров, или стрессеров, и этой атакой через этот ботнет существовала связь.

Что такое услуга бутера или стрессера? Это некий сайт, созданный какими-нибудь ребятами, которые заявляют, что продают вам услугу по проверке отказоустойчивости и стабильности ваших серверов. Вы платите определенную сумму и, как они утверждают, они якобы «отправляют такой-то объем трафика в течение такого-то

периода, чтобы вы могли протестировать свою инфраструктуру и понять, насколько она отказоустойчивая и может ли она устоять против атаки».

Но дело в том, что эти услуги бутера или стрессера продают эту услугу всем без исключения, вне зависимости от того, управляет ли этот человек проверяемой инфраструктурой или нет. Иными словами, они предоставляют услуги DDoS-атаки как наемники. И их легко найти. Можно зайти в интернет и выполнить простейший поиск в любимой поисковой системе, и вы их найдете. Кто-то из них настолько глуп, что принимает оплату банковскими картами, что упрощает работу светлой стороны. Все, что от вас требуется, — заплатить, а потом предоставить информацию, указав цель, которую вы хотите испытать, ведь, конечно же, вы просто хотите убедиться в отказоустойчивости сети. [неразборчиво] хорошо. Это совсем не круто.

Они делают это разными способами, и, конечно же, один из способов — использование ботнетов. Мы уже обсуждали технологию Fast Flux и Fast Flux с удвоенной скоростью. Я сказал про Avalanche. Мы это обсудим через пару слайдов. Avalanche — это вообще интересный случай, и вы поймете, почему.

Интернет вещей. Я не хотел произносить слово на букву «в», которое стоит между словами «интернет» и «вещей», но, к сожалению, это слово на букву «в» очень подходит сюда. И всем об этом давным-давно известно.

Хороший пример, как могут возникнуть проблемы: вспомните атаку, по-моему, против Брайана Кребса, вроде бы в октябре 2016 года. В сентябре? И против OVH, а это, между прочим, регистратор, аккредитованный ICANN. Также это крупный провайдер услуг хостинга во Франции. Они смогли определить, что источником атаки было примерно 146 000 цифровых видео-камер.

У ботнета была возможность отправить 1,5 терабайта данных. В то время это было просто неслыханно. Это же безумие. У меня такой объем данных даже в голове не укладывается. Фактический объем трафика, атаковавшего их, по оценкам составил 1,1 терабайт. Это были видеокамеры. Опять же, это не новость, но, мне кажется, об этом стоит упомянуть. DNS была одним из векторов, который использовался при атаке — не просто вектором, а полноценно использовавшимся вектором.

Еще есть WannaCry, о котором тоже будет сказано позже, так что пока не будем об этом.

Avalanche был облачным сервисом преступников. Представьте, что вы переходите на сайт, создаете

учетную запись, входите в нее и можете выбрать тип вредоносного ПО и тип кампании, которую хотите провести. А эти парни делали все остальное за вас. От вас требовалось только заплатить им, и они бы все сделали. Они бы предоставили вредоносное ПО для заражения клиентов. Они бы даже их сами заразили. Они бы [неразборчиво] доменное имя для управляющего сервера ботнета по вашему заказу. Они бы [неразборчиво] эти доменные имена для вас.

Они предоставляли хостинг для сайтов, распространяющих вредоносное ПО. Всем этим они бы управляли по вашему заказу. Так что это уже был новый уровень совершенства, если говорить о [испытании] преступных сервисов.

Avalanche, конечно, обеспечивал большую долю регистраций DGA на доменах, автоматически генерируемых по алгоритму. Когда правоохранительные органы начали принимать меры, соблюдался процесс ICANN — этот процесс называется «Ускоренный процесс подачи запросов об обеспечении безопасности регистратур». Посредством этого процесса из рук преступников было изъято 832 000 доменных имен.

То есть, от одной инстанции в другую, благодаря тесному сотрудничеству правоохранительных органов и

некоторых игроков частного сектора преступники полностью утратили управление над своей инфраструктурой. Оп! — и ее больше нет. Ну, в смысле, она есть, но для них она больше недоступна. Они не могут ей управлять. Как же приятно, когда такое происходит.

Вот некоторые строки, которые Avalanche, ботнет, должен был создать для использования управляющим сервером. Все эти 830 000 доменных имен должны были быть созданы в нескольких TLD, как ccTLD, так и gTLD. Как я уже сказал, преступники с удовольствием злоупотребляют всем, чем только можно. Разумеется, они не задумываются.

Итак, это один момент. Некоторые преступники в определенных странах создают вредоносное ПО таким образом, чтобы оно не атаковало IP-адреса в их собственных юрисдикциях, так как не хотят, чтобы правоохранительные органы их страны ими заинтересовались, ведь это может плохо кончиться. Так что они просто полностью пропускают собственное пространство IP-адресов.

И в этом случае, конечно, они не могут покинуть свою страну, что, конечно, само по себе хорошо. Они превращают себя в пленников собственных стран.

Хорошо, что они там и остаются, но ничего хорошего в том, что они наносят большой вред.

Это результат отключения Avalanche. Благодаря материалам, предоставленным Europol и ФБР, во всей презентации говорится только об этом одном случае. Это единственный результат. Пять арестов в четырех странах, 37 обысков в семи странах, 39 серверов изъято в 13 странах, 221 сервер отключен от сети, 64 TLD/832 000 доменов в 26 странах и огромная работа по возмещению ущерба для жертв, просветительская работа и меры по предотвращению. То есть это действительно крупномасштабная операция. Это хорошо. Это невероятный успех.

WannaCry была странным явлением, если рассматривать ее с точки зрения DNS. Она была интересна тем, что, в отличие от обыкновенных типов вредоносного ПО, которые используют доменные имена для управления внутри любого нормального TLD — gTLD или ccTLD — управление посредством WannaCry по большей части осуществлялось, по-моему, с семи доменов «.onion». Если вы помните «.onion», этот домен был классифицирован IETF как TLD специального назначения, то есть он никогда не окажется в корневой зоне, что значит, ICANN никогда и никаким образом не будет связана с «.onion». То есть не было способа

отключить управляющую инфраструктуру ботнета, связанную с WannaCry.

Тем не менее, один молодой исследователь, парень из Британии по имени Маркус Хатчинс, занимался анализом кода. Ему удалось получить образец WannaCry. Он его анализировал и наткнулся на некую строку в коде, если не ошибаюсь. Конечно она была жестко закодирована во вредоносном ПО. Он ее проверил. Она не была зарегистрирована. Он ее зарегистрировал и остановил распространение вредоносного ПО. По чистой случайности. Он и понятия не имел, что произойдет. Просто зарегистрировав это доменное имя, он остановил распространение вредоносного ПО.

Причина, по сути, в специфике структуры. Если моя программа-вымогатель подключена к управляющему серверу ботнета, то этот процесс позволяет избежать анализа. К счастью, именно так и оказалось. После этого распространение WannaCry было остановлено.

Тогда преступники, стоявшие за WannaCry, попытались зарегистрировать вторую строку, но ее также очень быстро зарегистрировали. В конечном итоге распространение было полностью остановлено. А они просто занялись чем-то другим.

Злоупотребление DNS вызывает большие дискуссии в ICANN. Существуют различные точки зрения. Кто-то, со стороны безопасности, со стороны правоохранительных органов, опасается насчет точности WHOIS и, разумеется, последствий GDPR для операций и структуры WHOIS после 25 мая, когда GDPR вступит в силу.

Кто-то опасается насчет времени ответа, времени реагирования в случае поступления данных о порте, через который происходят злоупотребления. С этим аспектом связано много разных опасений.

С другой стороны, и к этой стороне мы, как организация, также должны прислушиваться, существует опасение, что ICANN не сможет выйти за пределы своих полномочий или области работы, в том смысле, что, когда речь о содержимом, ICANN не должна иметь возможности на него влиять. Другими словами, в договорах ICANN нет положений, предусматривающих удаление, к примеру, содержимого, полученного пиратским путем. Эту тему должно обсуждать сообщество, а не организация. В целом, вот такие обсуждения вы, друзья, проводите. Мы содействуем их проведению, но не можем в них участвовать.

Что немаловажно, Рабочая группа по обеспечению общественной безопасности — это штаб, в котором правоохранительные органы, как гражданские, так и судебные, заседают в рамках структуры ICANN, допустим, более широкий спектр комитетов ICANN и так далее. До возникновения PSWG, в ее нынешнем виде, правоохранительное сообщество, по факту, не имело штаба, вплоть до, по-моему, Пекина, когда Лорин Капин из Федеральной торговой комиссии США не обратилась к Фади Шехади, бывшему генеральному директору, с просьбой рассмотреть возможность предоставления правоохранительным структурам официального места в структуре ICANN. Он парировал, обратившись к правоохранительному сообществу: «Жду от вас предложения». Они его и предоставили. Было предложено как раз создать известную нам PSWG, то есть рабочую группу или подгруппу в рамках Правительственного консультативного комитета. Вот где они заседают.

Предназначение PSWG — предоставлять рекомендации в GAC (Правительственный консультативный комитет) и, конечно, широкому сообществу ICANN. К темам, которыми они занимаются, относится злоупотребление DNS, естественно, способы использования доменных имен с преступными целями для нанесения вреда

пользователям, GDPR, так как они в любом случае повлияют на информацию в WHOIS, доступную для изучения и расследования угроз, а также передача операторского класса (CGN NAT). Вкратце, это технология, применяемая некоторыми интернет-провайдерами. Эта и подобные ей технологии используются некоторыми интернет-провайдерами, которые, по сути, не хотят переходить на IPv6.

Вместо перехода на IPv6 они создают огромные локальные сети и предоставляют своим пользователям внутренние IP-адреса. Есть IP-адреса, которые могут находиться только в интернете общего пользования, которые мы можем увидеть при анализе трафика, а их IP-адреса могут существовать только в частных сетях и не должны находиться в интернете общего пользования. Так происходит, например, в вашей компании или у вас в доме. Вашим устройствам назначаются частные IP-адреса.

А эти ISP назначают такие частные IP-адреса своим пользователям, будь их 500, 1 000 или 10 000 человек, и создают частные сети, охватывающие весь жилой район, со всего одним общедоступным IP-адресом. Это создает сложности для правоохранительных органов, ведь если их сотрудник, допустим, стучится в дверь с официальным документом или отправляет ISP повестку с вызовом в суд,

запрашивая информацию о пользователе, отправившем такой-то трафик с этого IP-адреса, в такой-то день и час, то ISP ответит: «Ну, я не знаю. К этому общедоступному IP-адресу относится 10 000 пользователей».

И во многих странах нет обязательных правил, или они есть, но не соблюдаются, по поводу обязанности по хранению данных, обслуживанию, а также хранению журналов регистрации трафика и входа/выхода из системы. То есть во многих странах вы можете войти в систему, потом выйти, и все! Данных нет. Никто не знает, что вы здесь были. ISP не знает, что вы здесь были. Все это очень сложно. Это одна из тем, которую в прошлом обсуждали в PSWG. Конечно, технологию Fast flux используют преступники.

Это очень простые примеры. Тут разумеется не идет и речи об обложении налогами или ограничениях — испытательные сроки в рамках договоров ICANN, более широкая сеть договоров, которые должны регулировать борьбу со злоупотреблениями. Есть много моментов. Мы можем много часов обсуждать борьбу со злоупотреблениями только с точки зрения договоров внутри ICANN.

Я могу заметить, что у регистратур все же есть обязанность контролировать свою зону на предмет угроз

безопасности. Это означат, что они обязаны наблюдать за доменами, которые существуют внутри них.

Если бы я был «.карлос» TLD, мне бы пришлось следить за всеми доменными именами «.карлос» и определять, где происходит фишинг, рассылка спама, вредоносного ПО и управление ботнетами, а потом отправлять эту статистику и показатели в ICANN. Это обязательство со стороны регистратур.

Также, если не ошибаюсь, по-моему, регистратуры также должны предоставлять контактные данные специалиста по борьбе со злоупотреблениями. Но, я думаю, в масштабах, связанных именно с противодействием злоупотреблениям в регистратурах.

При этом, со стороны регистраторов, все более конкретно. Эти более конкретные положения указаны в этом соглашении. Это соглашение называется «Соглашение об аккредитации регистраторов», или RAA, как мы его неофициально называем.

Эти более конкретные положения сформулированы на основании 12 рекомендаций правоохранительных органов, предоставленных теперь уже PSWG, а тогда это было просто правоохранительное сообщество, через GAC на конференции в Коста-Рике в 2012 году. По-моему, эти 12 рекомендаций были представлены именно тогда.

В результате Правление поручило персоналу начать переговоры с Группой заинтересованных сторон-регистраторов. Эти переговоры заняли несколько месяцев, и в итоге было составлено RAA 2013 года, включающее в себя некоторые более конкретные положения по поводу борьбы со злоупотреблениями.

Кто-то в сообществе оперативной безопасности по-прежнему хотел бы увидеть более четкие и жесткие положения, но в тот момент правоохранительные органы вполне устраивала формулировка, которую утвердили и Группа заинтересованных сторон-регистраторов, и организация ICANN.

Некоторые из этих обязанностей, если вкратце о них сказать, включают в себя, к примеру, обязанность регистраторов принимать оправданные меры в ответ на поступающие отчеты о злоупотреблениях. Конечно, если спросить 10 юристов, что означает «оправданные», то они дадут 20 разных ответов, и это усложняет ситуацию. Но вот так сказано в RAA.

Другая обязанность — они также должны предоставлять контактные данные специалиста по борьбе со злоупотреблениями. По-моему, эти данные должны публиковать на сайте и/или в данных WHOIS. Обычно это входит в данные WHOIS, по-моему. Также они должны это

публиковать на своем сайте. Я, правда, не уверен. По-моему, это должно быть там указано, но я не уверен.

Есть одно интересное положение, относящееся конкретно к правоохранительным органам. Если правоохранительная структура из одной юрисдикции с регистратором отправляет отчет о злоупотреблении этому регистратору — и они должны быть именно в одной юрисдикции — регистратор обязан предоставить не автоматический ответ в течение 24 часов. Это, как я сказал, не может быть автоматически генерируемый ответ. Ответ не обязательно должен выглядеть как «Мы приостановили работу домена». Это может быть просто ответ «Принято к сведению/Мы подтверждаем получение». Это допустимый ответ.

Право отправки этого ответа, согласно положениям соглашения, может быть предоставлено только лицам, способным принимать решения о дальнейших действиях в отношении отчета о злоупотреблениях, о том, будет или не будет приостановлена работа домена.

В некоторых юрисдикциях это положение оказывается очень действенным, если к ним относится много регистраторов, но есть некоторые юрисдикции, где регистраторов мало или вообще нет. И, конечно же,

эффективность или результаты применения этого положения зависят от юрисдикции.

Поставщик услуг сохранения конфиденциальности и регистрации через доверенных лиц: если помните, эти услуги, к которым прибегают владельцы доменов, чтобы в WHOIS в связи с их доменным именем была размещена информация о ком-то другом, а не о них. Если у меня есть сайт, и я не хочу, чтобы мое имя где-то фигурировало, или мой адрес, или электронная почта, то поставщики таких услуг, которыми также управляют регистраторы, также должны предоставить собственные контактные данные специалиста по борьбе со злоупотреблениями.

Я думаю, что это все. Таковы темы, которые мы сегодня должны были обсудить. Информации много. Как я говорил, хотя злоупотребление DNS кажется ясным и понятным, когда, допустим, есть доменное имя, используемое для управления ботнетами, то понятно, что и как. Как только вы его видите, вы можете провести технический анализ и получить неоспоримые технические, научные доказательства, показывающие, как обстоит дело. Но не все случаи настолько конкретны.

Так что эта тема нуждается в дальнейшем обсуждении. Сообщество должно и дальше развивать и расширять эти темы.

Наша задача — я забыл про это сказать в самом начале. Я директор по взаимодействию по вопросам безопасности, стабильности и отказоустойчивости в Группе по безопасности, стабильности и отказоустойчивости. Мы относимся к офису технического директора. Мы активно сотрудничаем с сообществом, которое занимается вопросами оперативной безопасности, а также с правоохранительными органами.

У нас множество целей. Мы стараемся сделать их ближе ICANN. Мы бы очень хотели, чтобы там понимали суть обсуждений, которые здесь ведутся. Всего пару недель назад представитель доменной отрасли по нашему приглашению посетил конференцию по вопросам безопасности. Речь о Рабочей группе по противодействию компьютерным злоумышленникам в области передачи сообщений. Это был Джонатан Фрэйкс, исполнительный директор ассоциации доменных имен. Для него встреча прошла плодотворно.

Это одно из направлений нашей работы. Мы вовлекаем людей. Мы стремимся объединить людей, которые могут по привычке рассматривать друг друга как противников из разных лагерей. Мы стремимся, чтобы они поняли друг друга. Ели они смогут понять мотивы другой стороны, то на этом фундаменте можно будет что-то построить.

Мы обучаем правоохранительные органы. Одной из обязанностей ICANN, как вы можете помнить, является содействие в обеспечении безопасности, стабильности и отказоустойчивости системы доменных имен. Это значит, что правоохранительные органы должны понимать, что происходит, когда они наблюдают за расследованием в отношении ботнета, или когда они наблюдают за расследованием в отношении распространения вредоносного ПО. Они должны понимать, как работает DNS. Мы помогаем им понять это, так чтобы они могли обеспечивать SSR системы, как мы это называем, да, очередная аббревиатура.

Я думаю, что это все. И если у кого-то есть вопросы, пожалуйста, не стесняйтесь.

КАТИ ПЕТЕРСЕН: Напоминаю, что необходимо назвать свое имя, и кого вы представляете, если это актуально.

[МАРСИ СУРМО (MARSY SURMO)]: Здравствуйте. Я [Марси Сурмо] из Индии. [неразборчиво] также вопрос: подготовила ли ICANN некие базовые стандарты безопасности для реализации или функционирования DNS. Можно ли ее поддерживать каким-то иным способом? Речь может идти

об операционном устройстве, которое никак не защищено. Будут происходить все возможные злоупотребления. И анализ будет проводиться только пост-фактум. Так что можно ли ввести некие минимальные базовые стандарты безопасности в отношении любой работающей DNS?

КАРЛОС АЛВАРЕЗ: Я предлагаю вам обратиться к документам, опубликованным DNS-OARC, сообществом операторов DNS. Конечно, естественно, стандарты IETF, которые могут включать положения о безопасности, касающиеся DNS. Также обратитесь к M3AAWG. Примерно полтора года назад они обновили так называемое...забыл название. Обратитесь к материалам M3AAWG по угрозам DNS, вы все найдете. Я уверен. Они в целом содержат ценную информацию.

Вот эти сообщества или группы, я думаю, занимались разработкой и составили документы или стандарты, о которых вы говорите.

[МАРСИ СУРМО]: Это просто указания. Можно просто [неразборчиво] об этом до перехода к [неразборчиво] этих устройств, эти минимальные стандарты безопасности будут внедрены?

КАРЛОС АЛВАРЕЗ: Это нельзя сделать в принудительном порядке. Кто угодно может настроить, запустить и контролировать DNS-сервер. Кто угодно в мире. Это невозможно сделать принудительно. Это технически невозможно предотвратить. Нет правила. Нет обязательной силы. Любой может поступать так. Это все на добровольной основе, и потому весьма сомнительно.

Отвечая на ваше высказывание, насчет добровольности всего этого, есть стандарты и механизмы выполнения действий, установленные техническим сообществом много лет назад, например, с 1997 года действует правило фильтрации четвертых IP-адресов. Если вы обратитесь к BCP 38 или BCP 84, то увидите, то эти передовые методики говорят о 20 и более годах. Да, из-за того, что все это добровольно, они применяются не так широко, или не так широко, как хотелось бы. Все добровольно.

Другие вопросы?

Да, прошу.

[ХАРУ АЛЬ ХАССАН (HARU AL HASSAN)]: На самом деле...

КАРЛОС АЛВАРЕЗ: Ваше имя и кого вы представляете.

[ХАРУ АЛЬ ХАССАН]: Меня зовут [Хару аль Хассан], я из Нигерии. В развивающихся странах нам приходится сталкиваться с такими проблемами: как обучить правоохранительные органы, чтобы они могли бороться с преступниками? Вы показали много способов заражения DNS, атаки DNS, так как нам обучать правоохранительные органы, чтобы они могли бороться с преступниками?

КАРЛОС АЛВАРЕЗ: Я считаю, что правильно будет обратиться в отдел взаимодействия ICANN в Африке. То есть к Пьеру. Не знаю, может быть вы уже знакомы. Обсудите свои вопросы с ним.

Тогда Пьер, совместно с группой по SSR, будет координировать участие правоохранительных органов в обучении, посвященном злоупотреблению DNS. То есть предлагаю вам обратиться к Пьеру, так как вопрос действительно актуальный.

Да, прошу.

БРЕНТ КЭРИ (BRENT CAREY): Брент Кэри из .nz. Мне хотелось бы узнать, есть ли у вас какие-то завязки по поводу интернета и юрисдикции. Я на прошлой неделе вернулся из Оттавы, там возникло напряжение по поводу доменных имен. Очевидно, злоупотребление инфраструктурой, злоупотребления при регистрации, злоупотребления, связанные с содержимым, — все сливается воедино. Я только надеялся, что у вас есть какие-то завязки по этому поводу.

КАРЛОС АЛВАРЕЗ: Нет. Вот так-то. Но, да, я знаю, что мы пытались организовать этот форум в Оттаве. Кто-то из моих коллег из ICANN там присутствовал.

БРЕНТ КЭРИ: Просто отсутствие представителей правоохранительных органов было очень заметно.

КАРЛОС АЛВАРЕЗ: Хорошо. Я не знал. Может быть, стоит это обсудить с PSWG. Спасибо.

БРЕНТ КЭРИ: Спасибо.

КАРЛОС АЛВАРЕЗ: Хорошо. Итак, остался еще один.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Прямо вдогонку] я [не] сказал бы, что мы располагаем стабильным механизмом [неразборчиво] этих GDPR для WHOIS. То есть мы не можем управлять этими проблемами безопасности. Впереди возникнут сложности, похоже.

КАРЛОС АЛВАРЕЗ: Какие сложности?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: С одной стороны, у нас нет аутентичного WHOIS. А эти GDPR, возможно, не позволят нам видеть, кто к нам обращается, и куда мы движемся.

КАРЛОС АЛВАРЕЗ: Верно.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Во-вторых, не обеспечена безопасность DNS. Мы ей не управляем. То есть, мы движемся в ту сторону, где отсутствуют возможности контроля и проверки аутентичности человека.

КАРЛОС АЛВАРЕЗ: Давайте подождем. Я предлагаю вам участвовать в этих обсуждениях и озвучивать свое мнение, когда организация ICANN делает соответствующие призывы. Обычно этим занимается генеральный директор, который в последнее время постоянно призывает людей предоставлять обратную связь. Так что обязательно участвуйте, ведь именно так ваш голос будет услышан. На самом деле, мы его слышим. Это не фигура речи. Мы его слышим. Так что сообщайте о своих опасениях туда. Это правильное место.

Есть заседания. Это заседание ни в коем случае не единственное, связанное со злоупотреблением DNS. Просто имейте это в виду. Если бы можно было отмотать время назад, вы могли бы посетить вчерашнее заседание о прогрессе PSWG в 11:30. А завтра в 8:30 пройдет совещание GAC PSWG. Я рекомендую вам посетить их с утра.

Да, я более положительно настроен в отношении GDPR, просто сейчас такой момент. Но оба совещания будут интересными.

Будет интересно посмотреть, как доменная отрасль поступает в отношении собственной инициативы Healthy Domains. Приятно наблюдать за тем, что они делают, так как они делают нечто интересное.

DAAR — это инструмент, разработанный моей группой. Он позволяет узнать информацию о неблагополучных регистрациях и их накоплении в одной области по сравнению с другими областями. Это тоже будет интересным. Не буду подробно про это рассказывать, так как хочу, чтобы вы посетили это заседание. Просто приходите. Приходите, и вам не будет скучно.

Хорошо. Итак, благодарю всех, кто пришел.

КАТИ ПЕТЕРСЕН: В качестве напоминания: слайды презентации для этого заседания уже в открытом доступе. Мы дополним их расшифровкой выступления, а также записью этого заседания через пару дней. Так что вы сможете вернуться и еще раз все пересмотреть.

Большое спасибо. Следующая сессия по принципам работы, посвященная работе с сетью интернет, пройдет в 3:30. Не в 3:15, а в 3:30. Извините, мы немного задержимся со следующей сессией по принципам работы. Сессия по работе с сетью интернет будет в большой степени посвящаться протоколам IPv4 и IPv6.

Надеюсь, что вы останетесь, попьете кофе и снова вернетесь к нам. Спасибо.

[КОНЕЦ СТЕНОГРАММЫ]