ICANN82 | Форум сообщества - Совместное заседание: GAC и SSAC
Воскресенье, 09 марта 2025 года - 16:30 - 17:30 PST

NICOLAS CABALLERO: Дамы и господа, приветствуем вас снова. Мы начинаем. Пожалуйста, займите свои места. Джулия, пожалуйста, начните запись.

GULTEN TEPE: Здравствуйте, приветствуем вас на заседании GAC и SSAC на ICANN82 в воскресенье, 9 марта, в 16:30 по местному времени. Пожалуйста, обратите внимание, что заседание записывается и регулируется Ожидаемыми стандартами поведения ICANN и Политикой борьбы с домогательствами сообщества ICANN.

Во время заседания вопросы и комментарии, заданные в чате, будут зачитаны вслух, если они будут заданы в соответствующей форме. Пожалуйста, не забудьте указать свое имя и язык, на котором вы будете говорить, если вы будете говорить не на английском. Пожалуйста, говорите четко и в разумном темпе, чтобы обеспечить точный перевод, и не забудьте отключить звук всех других устройств, когда вы говорите. Вы можете получить доступ ко всем функциям этого заседания на панели инструментов Zoom. На этом я

предоставляю слово Николасу Кабальеро (Nicolas Caballero), председателю GAC. Спасибо. Вам слово, Нико.

NICOLAS CABALLERO Спасибо большое, Гюльтен. Приветствую всех на последнем, но самом важном, по моему скромному мнению, заседании с SSAC, Консультативным комитетом по безопасности и стабильности. Приветствую вас, Рам. Приветствую вашу замечательную команду. Собственно говоря, мы обсуждали некоторые из вопросов, о которых будем говорить сегодня, вчера и позавчера. И когда я упомянул квантовые вычисления и их потенциальное влияние на DNS, стабильность DNS, реализацию DNSSEC и так далее, а также криптографию в целом, симметричную и асимметричную, все посмотрели на меня как на сумасшедшего, что, возможно, так и есть. Но, как бы то ни было, мы будем подробно говорить об этом с этой командой экспертов. Мы затронем тему квантовых вычислений и их влияния на шифрование, как я уже говорил вчера.

Затем мы обсудим Infermal. К сведению 60 новых членов GAC, я уже объяснил, что означает Infermal. Но мы перейдем к деталям. А затем мы обсудим дальнейшие шаги. Так что еще раз приветствую вас, Рам, и вашу потрясающую команду. Слово за вами.

RAM MOHAN

Нико, спасибо вам большое. И от имени SSAC я выражаю искреннюю благодарность GAC за это приглашение. Мы встречаемся с вами уже в третий раз. И с каждым разом наше общение становится все более насыщенным и интересным. Мы очень ценим эту возможность укрепить наш совместный диалог по важнейшим вопросам безопасности и стабильности интернета.

Для тех из вас, кто впервые работает в GAC и в сообществе ICANN, коротко расскажу, что SSAC является экспертным консультативным органом ICANN. Его задача - выявлять и анализировать потенциальные угрозы для систем именования и адресации в Интернете. В состав SSAC входят опытные технические специалисты. Мы предоставляем объективные, основанные на фактах рекомендации сообществу и Правлению ICANN.

Бывают случаи, когда мы не даем рекомендаций, основанных на фактах. В таких случаях мы стараемся подчеркнуть, что это экспертные мнения, которые мы представляем сообществу и Правлению. Наша деятельность охватывает широкий спектр вопросов: от уязвимостей DNS и рисков кибербезопасности до влияния новых технологий на инфраструктуру интернета и аспектов безопасности, стабильности и отказоустойчивости управления интернетом. Так что мы занимаемся всем этим. Но в основном наша сфера деятельности лежит в области критической инфраструктуры. И мы работаем в этой области.

Мы понимаем, что GAC играет важную роль в представлении правительственных взглядов на управление интернетом, среди прочего. И это взаимодействие, Нико, это взаимодействие действительно позволяет нам из SSAC соединить техническую и политическую сферы, и наше желание и стремление продолжать это взаимодействие заключается в том, чтобы наши рекомендации были надежными и соответствовали общественным интересам. Так что это ключевое направление нашей работы. Мы готовы поделиться своими соображениями, выслушать вашу обеспокоенность и вместе внести вклад в создание безопасного, стабильного и устойчивого Интернета.

Так что это действительно ключевая движущая сила нашей работы, и поэтому мы очень дорожим этим взаимодействием с GAC. Спасибо за это. Как вы уже сказали, у нас есть две ключевые темы, которые мы хотели бы обсудить с вами. Справа от меня сидит Расс Хаусли (Russ Housley). У Расса долгая и выдающаяся карьера. Среди прочего он уделяет много времени изучению квантовых вычислений и их влияния на шифрование. Так что мы решили пригласить Расса, чтобы он поделился своими мыслями на эту тему. Мы не собираемся читать вам лекции. Мы хотим поделиться своими мыслями, а затем попросить вас принять участие в обсуждении, пообщаться с нами.

Мы стараемся, насколько это возможно, не делать наши презентации чрезвычайно техничными, хотя материал,

который в них содержится, очень техничен. В этом и состоит наша цель. Так что, если мы будем переходить исключительно на язык гиков, просто скажите: «Эй, что это значит? Мы будем рады перевести это. Так что, вам слово, Расс.

RUSS HOUSLEY

Спасибо, Рам. Итак, я поместил зацепку прямо на титульный слайд. Пока никто не знает ответа. Квантовые вычисления появились уже давно. И Национальный институт стандартов и технологий провел большое соревнование. И решение, которое появилось в результате, называется ML-DSA. Это алгоритм цифровой подписи на основе решетки. И это решение просто не подходит для DNSSEC. Оно просто слишком большое. У него очень большие открытые ключи и очень большие значения подписи, так что, если вы используете DNS через UDP, он не подходит. Все просто.

Хорошая новость заключается в том, что у нас еще есть время. Потому что самая большая обеспокоенность в связи с квантовыми вычислениями — это то, что мы называем атакой «собери сейчас, расшифруй потом». Так что обеспокоенность заключается в том, что если у вас есть куча секретов, а злоумышленник записывает их и сохраняет до тех пор, пока у него не появится криптографически релевантный квантовый компьютер, то он сможет атаковать управление ключами с помощью квантового компьютера, получить ключи и расшифровать секреты. В DNS нет никаких секретов, так что

это не проблема. Наша обеспокоенность заключается в том, чтобы у нас была цифровая подпись, которую нельзя будет подделать со временем, когда нам понадобится смягчить последствия появления квантового компьютера.

Итак, на втором слайде я рассказываю о том, что возможно сделать для применения этих квантовых цифровых подписей. В настоящее время ведутся исследования. В Инженерной исследовательской группе интернет-технологий есть группа, изучающая пост-квантовый DNSSEC. Ее заседание состоится на следующей неделе. Дерево хешей, похоже, является основой ответа. Оно является ответом на многие вопросы, включая блокчейн, транспарентность сертификатов и целый ряд других технологий. Так что, возможно, нет ничего удивительного в том, что они лежат в основе. Но я поместил здесь на слайде несколько ссылок.

В одной из них говорится о том, как могут быть применены подписи на основе хэш-памяти с состоянием, что эти подписи также велики, так что они рассматривают другие методы. В любом случае, на следующей неделе на IETF 122 будет много дискуссий, чтобы изучить эти вопросы. Но я не ожидаю ответа через год. Но у нас есть время. Так что, если у вас есть вопросы по этому поводу, или мы отложим их до конца, или вы хотите задать их сейчас? Хорошо, если у вас есть вопросы, я буду рад ответить.

NICOLAS CABALLERO Спасибо. Спасибо вам большое. Можно задать вопросы. Я хотел бы, чтобы вы объяснили, опять же, для полного состава GAC, что такое цифровые подписи, ванильная версия, что такое цифровые подписи, пожалуйста.

RUSS HOUSLEY Конечно. Цифровая подпись — это то, на чем держится DNSSEC. Идея заключается в том, что, когда вы получаете ответ на свой запрос, к нему прикрепляется цифровая подпись. А это означает, что он не был изменен с момента первоначального размещения. Так что именно она обеспечивает целостность и подлинность самих данных.

NICOLAS CABALLERO Спасибо вам большое. У меня Нидерланды.

MARCO HOGEWONING Спасибо, господин председатель. Для протокола, это Марко из Нидерландов. Спасибо за этот очень краткий, но глубокий обзор. Я согласен. Нам еще предстоит пройти долгий путь. Тем не менее, я являюсь представителем правительства. И я знаю, что долгий путь часто короче, чем вы думаете. Не вдаваясь в технические подробности, есть ли какие-то конкретные рекомендации, которые вы могли бы дать нам, правительствам, прямо сейчас? И что мы можем сделать, чтобы подготовиться к тому, что, вероятно, станет

неизбежным моментом, когда нам придется изменить алгоритм DNSSEC?

RUSS HOUSLEY

Для DNSSEC еще слишком рано. Для других протоколов безопасности у нас есть решения. Мы работаем в других рабочих группах IETF, таких как LAMPS, которая работает над PKI и SMIME. У нас есть TLS. И у нас есть IPSEC в этих трех областях. Простите, и Secure Shell. В этих четырех областях у нас есть решения, где инфраструктура должна быть развернута уже сейчас, так чтобы, когда она нам понадобится, она уже имелась. Потому что на это уйдет несколько лет.

Если вспомнить переход от SHA-1 к SHA-256, то в то время я был директором IETF по безопасности и думал, что пяти лет будет достаточно. А потребовалось более чем в два раза больше. Так что начните с инфраструктуры, чтобы переход мог состояться, потому что куча вещей потом не сможет произойти, если не будет инфраструктуры, к которой их можно привязать. Это моя рекомендация.

NICOLAS CABALLERO

Стив, Вам слово, пожалуйста.

STEVE CROCKER

Спасибо. Расс, наверное, было бы неплохо ответить на этот вопрос, который имеет большой смысл, когда правительство говорит: «Что мы будем делать? Вы упомянули о предыдущем

переходе от SHA-1 к SHA-256. Можете ли вы сказать что-нибудь о том, как будет выглядеть переход в тот момент, когда будет принято решение о том, как будет выглядеть новый алгоритм? Будет ли переход на этот новый алгоритм качественно отличаться от всех тех смен алгоритмов, которые уже были и будут на нашем пути, или это будет еще одна смена алгоритма, для выполнения которой у нас уже есть определенная практика и опыт?

RUSS HOUSLEY Спасибо, Стив. Мы не знаем точно ответ, но знаем, что этот вариант сложнее, потому что мы не просто меняем одну из деталей коробки передач. Мы выкидываем всю коробку передач и ставим новую. Так что, думаю, в этой ситуации нужно думать о том, что если вы думаете о PKI, то вы говорите о создании новой системы от корня до конца. Вы не просто меняете ее части. Надеюсь, это помогло. Нет? Извините.

NICOLAS CABALLERO Спасибо, Стив, за вопрос. Спасибо, Расс. Есть еще вопросы или комментарии? У меня есть вопрос к вам, Расс. Допустим, у определенного правительства очень хорошая реализация DNSSEC, MANRS, RPKI и так далее и тому подобное. Любая комбинация Blowfish, RSA и, я не знаю, DES или что-то еще, SHA-256 или любая другая комбинация, и вдруг происходит прорыв в квантовых вычислениях. Поправьте меня, если я

ошибаюсь, но в этом случае правительство, инфраструктура DNSSEC автоматически устареют. Я прав?

RUSS HOUSLEY

Да. Однако неизвестно, когда это произойдет. Сейчас мы видим много литературы о том, как увеличивается количество кубитов и размер квантового компьютера. Но пока что мы и близко не подошли к чему-то криптографически значимому. И эти вещи не являются линейными.

Прогресс происходит скачками и рывками. Так что, когда это произойдет, мы не обязательно получим много предупреждений, и в этом смысл ответа, который я дал предыдущему человеку. Но RPKI и DNSSEC уникальны тем, что в них требуется только целостность. Там нет проблем с добычей секретов. Так что у нас есть больше времени, потому что нет обеспокоенности типа «запиши сейчас, собери потом» или «собери сейчас, расшифруй потом».

NICOLAS CABALLERO

То есть нам вполне достаточно хорошего сочетания DNSSEC, RPKI и MANRS.

RUSS HOUSLEY

Верно. У нас просто больше времени на эти проблемы, потому что они связаны только с публичными данными и обеспечением их целостности.

NICOLAS CABALLERO Спасибо, Расс. У меня Австралия и Нидерланды. Австралия, пожалуйста, вам слово.

INGRAM NIBLOCK Здравствуйте. Ингрaм Ниблок (Ingram Niblock) от Австралии. Я знаю, что они служат разным целям. Но я просто хотел узнать, не могли бы вы прокомментировать роль DNS по HTTPS и DNS по TLS. Очевидно, что один подписывает, а другой обеспечивает транспортную безопасность. Но будет ли проще реализовать постквантовое шифрование, новые алгоритмы в средствах защиты транспорта, и даст ли это какие-либо преимущества, которые мы сейчас получаем от DNSSEC в силу того, что шифрование осуществляется и в транспорте?

RUSS HOUSLEY И да, и нет. Да, они будут защищать трафик между точкой шифрования и точкой дешифрования. Это система hop-by-hop, когда вы применяете ее к DNS. Так что это обеспечит защиту. Как я уже сказал, работа над TLS продолжается. У нас еще нет PKI, к которой он будет подключен. Кстати, на следующей неделе после IETF в Токио состоится форум браузеров CA, на котором будет обсуждаться именно эта тема. Так что, надеюсь, это ответило на ваш вопрос.

NICOLAS CABALLERO

Спасибо, Австралия. Спасибо, Расс, еще раз для новых членов GAC: PKI означает «Инфраструктура открытых ключей», а MANRS - «согласованные нормы обеспечения защищенности маршрутизации». В любом случае, мы можем предоставить ссылки и все остальное. У меня Нидерланды, а затем джентльмен вон там. Извините, я не знаю вашего имени, но сначала Нидерланды.

MARCO HOGEWONING

Спасибо, господин председатель. Это снова Марко. Я немного отклоняюсь от темы и, возможно, пытаюсь избежать технической дискуссии. Но на предыдущем слайде вы упомянули о вызовах, связанных с транспортом UDP. Помнится, это уже не первый случай, когда в отрасли DNS мы сталкиваемся с ограничениями при использовании UDP в качестве транспорта.

Я полагаю, что это также играет роль в текущих реализациях DNSSEC в отношении длины ключа. Мне интересно, и это немного созвучно тому, о чем только что спросил мой австралийский коллега, учитывая, что мы смотрим на долгосрочную перспективу, можно ли рассмотреть различные варианты транспортировки DNS, кроме UDP?

RUSS HOUSLEY Другие варианты транспортировки хорошо понятны и определены, просто они не так хорошо внедрены. Так что в рамках этого перехода, возможно, они будут.

MARCO HOGEWONING Это снова возвращает нас к вопросу: мы правительства, как мы можем помочь?

RUSS HOUSLEY Весьма справедливо.

NICOLAS CABALLERO Росс, в этой связи не могли бы вы привести два-три примера?

RUSS HOUSLEY Два-три примера?

NICOLAS CABALLERO Для замены UDP я имею в виду.

RUSS HOUSLEY DNS через TCP, DNS через QUIC - это DNS через TLS. Вот примеры тех, которые не имеют таких ограничений на количество сообщений.

NICOLAS CABALLERO Спасибо большое. Нидерланды?

PETER THOMASSEN

Здравствуйте, это Питер Томассен (Peter Thomassen). Я также являюсь членом SSAC, и мне показалось, что некоторые вещи, которые были сказаны, можно пересказать в менее техническом ключе. Так что именно это я и пытаюсь сделать. Росс уже говорил, что подписи прикрепляются к ответам DNS, и они свидетельствуют о том, что информация DNS не была изменена с момента ее публикации. Конечно, если бы каждый мог просто прикрепить подпись, это было бы не очень полезно.

Таким образом, чтобы прикрепить подпись, необходимо иметь контроль над закрытым ключом, который нужен для вычисления подписи. Угроза со стороны квантовых компьютеров заключается в том, чтобы каким-то образом извлечь этот ключ, даже если вы не имеете права его иметь, и тогда вы сможете подделать эти подписи.

Еще одно применение криптографии - шифрование, которое позволяет защитить секретные данные и сделать их нечитаемыми, если у вас нет ключа для расшифровки. Так что это тоже применение ключей. И важно признать, что квантовые вычисления угрожают обоим применениям, как вычислению подписей с секретными ключами, так и расшифровке шифров. Но это разные случаи использования, а DNS не занимается шифрованием и дешифрованием. Его задача - проверить в момент, когда вы пытаетесь куда-то

подключиться и делаете DNS-запрос, действительна ли та подпись, которую вы получаете, в данный момент.

Так что если вы захотите взломать его с помощью квантового компьютера, вам придется сделать это за очень короткий промежуток времени, почти в реальном времени, в то время как если вы записали зашифрованную информацию, например передачу данных по протоколу HTTPS в прошлом, вам понадобится около пяти лет, чтобы расшифровать ее, если вы захотите. Так что если у вас есть полезный, но медленный квантовый компьютер, он будет угрожать вашим зашифрованным данным, но он не будет угрожать в это время вашей информации DNSSEC, потому что, если потребуется пять лет, чтобы подделать подпись, к тому времени ответ DNS уже никого не будет интересовать, верно? Потому что ваше соединение занимает всего несколько секунд.

Таким образом, суть в том, что, как и то, что правительства могли бы сделать сейчас, а это, я думаю, вопрос, заданный Нидерландами по поводу DNSSEC, не стоит пугаться. В настоящее время это исследовательская проблема. Полагаю, если вам это интересно, неплохо было бы проследить за этим. Но более насущной проблемой, безусловно, является защита хранимых или передаваемых секретных данных, которая имеет те же проблемы с извлечением ключа, но она гораздо более актуальна, и в ней уже достигнут больший прогресс, чем

в области DNSSEC. Да, так что это было то резюме, которое я хотел сделать.

NICOLAS CABALLERO Большое спасибо.

RUSS HOUSLEY Спасибо, что председательствуете на заседании на следующей неделе.

RAM MOHAN Спасибо, Нико. Я хотел бы предложить вам, Нико, и GAC одну вещь: если вам будет полезен какой-то готовый отчет, что-то вроде букваря в этой области, напишите нам, и мы поможем предоставить вам материал, который, возможно, будет полезен вашим членам, когда вы будете работать с вашими правительствами. Я думаю, что есть полезное различие, которое нужно понимать и передавать другим в ваших правительствах о том, что является отрицательной стороной квантования и DNSSEC по сравнению с отрицательной стороной квантования и общих секретов.

NICOLAS CABALLERO Спасибо вам большое. Рам, и спасибо вам, Расс. Я не уверен, я не совсем уверен по поводу упомянутого вами пятилетнего периода. Я забыл его имя. Питер, но спасибо за объяснение. Я действительно думаю, что мы можем, надеюсь, что нет, но у

нас могут быть сюрпризы в ближайшем будущем. В любом случае, прежде чем я передам слово Джеффу, есть ли у нас еще вопросы в зале или онлайн? Я не вижу ни одной поднятой руки. Спасибо вам большое, Расс. Так что давайте продолжим. И сейчас я передаю слово Джеффу, вам слово.

JEFF BEDSER

Спасибо, Нико. Джефф Бедсер (Jeff Bedser) от SSAC. Вопрос был задан для обсуждения исследования INFERMAL, исследования INFERMAL. Следующий слайд, пожалуйста. Спасибо. Исследование INFERMAL — это исследование, проведенное OCTO, офисом технического директора ICANN, в рамках их исследовательского компонента. В нем участвуют ученые, которые изучают вредоносные регистрации, когда речь идет о доменах, используемых для причинения вреда и злоумышленных доменов онлайн, в первую очередь фишинга.

И первое, о чем следует предупредить, и я выделил это жирным шрифтом во втором абзаце, — это не отчет, предлагающий решения, а отчет, призванный ответить на вопросы, которые уже давно задаются сообществом, о влиянии определенных факторов на то, где киберпреступники получают свои домены для подобных злоумышленных целей. В отчете говорится об экономических стимулах, проактивной проверке и некоторых строгих ограничениях в борьбе со злоупотреблениями доменами,

которые были приняты на момент выхода отчета в ноябре прошлого года.

Некоторые из основных выводов, для тех из вас, кто не читал отчет, касаются экономических стимулов: снижение оплаты регистрации, каждый доллар снижения оплаты соответствует 49%-ному увеличению злоумышленных доменов, бесплатные услуги или доступность таких услуг, как веб-хостинг, повышают уровень злоумышленных доменов на 88%. Скидки на регистрацию доменов связаны со значительным увеличением числа вредоносных регистраций. Что касается упреждающих мер, то строгие ограничения для тех, кто покупает домены, могут снизить злоупотребления на 63 %.

Доступ к API, то есть возможность совершать большие объемы массовых покупок доменных имен за один раз, может привести к увеличению числа регистрируемых вредоносных доменов на 401 %, и, конечно, практика проверки, проактивная проверка информации о владельце домена, например, проверка электронной почты и номера телефона, значительно снижает количество вредоносных регистраций. Следующий слайд, пожалуйста.

Реактивные меры, время смягчения последствий, влияние времени смягчения последствий на снижение злоупотреблений доменами минимально. Даже кратковременное восстановление может дать злоумышленникам возможность получить ценные учетные

данные и финансовую выгоду. Затем предпочтения регистраторов и TLD, концентрация злоупотреблений, вредоносные регистрации распределены неравномерно и, как правило, сосредоточены у определенных регистраторов и TLD, а практика регистраторов, например, предлагающих низкие цены и бесплатные услуги, с большей вероятностью привлекает вредоносные регистрации.

Это подтвержденная информация, которая давно и хорошо известна в сообществах по борьбе со злоупотреблениями. Проблема просто в том, что это экономический подход. Покупатели идут за самой дешевой ценой. Покупатели идут туда, где можно купить оптом. Я думаю, что в большинстве стран мира сейчас есть крупные организации, которые продают оптом все виды продуктов и товаров и продают их по самой низкой цене. Так что, хотя такое прочтение данных вполне оправданно, оно не обязательно подразумевает решение проблемы, поскольку если вы поднимете нижнюю границу цены, у вас все равно останется самая низкая цена. Если вы не зафиксируете цены на всей планете с разными экономиками и разными валютами, вы не устраните эту проблему.

Кроме того, убытки от киберпреступлений - я видел цифры от 1 триллиона долларов в год до 10 триллионов долларов в год. Я, конечно, понимаю, что между этими двумя цифрами не хватает нуля, но я даже не могу представить себе триллион долларов. Таким образом, разница между 1 триллионом и 10

триллионами долларов, если говорить об убытках, — это очень большая цифра. Большинство исследований показывают, что во всем мире средний ущерб от одного фиша на одну жертву составляет 136 долларов. Однако в Соединенных Штатах эта цифра возрастает до 3 500 долларов.

Я видел варианты всех этих цифр, и я уверен, что большинство людей, которые занимаются борьбой со злоупотреблениями, знают, что эти цифры варьируются в зависимости от исследования и т. д. Но реальность такова, что если каждая потеря составляет как минимум 136 долларов, то какая цена должна быть установлена за домен, чтобы было экономически нецелесообразно покупать домен, чтобы использовать его для нанесения вреда, если вы зарабатываете значительные суммы денег на киберпреступности? Это повод для размышлений, потому что мы рассматриваем, какие меры, какие изменения должны быть приняты, чтобы снизить или уменьшить проблему вредоносных регистраций, используемых для киберпреступлений, причинения вреда людям и кражи у них денег.

Изменит ли изменение цены стимул преступника зарабатывать сотни тысяч долларов, если домен подорожает с 2 до 10 долларов в год? Я задал этот вопрос. Процесс проверки, опять же, как я уже отмечал, был опубликован в ноябре, и исследование было основано на данных того времени. И проблемы ИИ, искусственного интеллекта,

продолжают ускоряться темпами, которые, очевидно, превышают темпы развития квантовых технологий.

Но возможность создавать цифровые идентичности, когда вы можете взять чье-то настоящее имя, сказать алгоритму искусственного интеллекта: «Мне нужны водительские права из этого конкретного региона этой конкретной страны, точный формат, но мне нужно имя реального человека, который принадлежит к этой возрастной категории и имеет фотографию, похожую на мою, или наклеить на него мою фотографию, чтобы иметь возможность в цифровом виде сгенерировать идентификатор, который затем можно использовать в процессе регистрации домена. Это действительно значительно повлияло на возможность сказать: «Ну, если бы они просто проверяли идентификатор каждого владельца домена, они могли бы решить эту проблему».

Способность отличить подделку от настоящего, когда это реальный человек с неправильной или похожей фотографией, достигает такого уровня, что для борьбы с ней приходится использовать искусственный интеллект, потому что человек не может сделать это на таком уровне и с такой скоростью, как это необходимо. Так что какие процессы помогут уберечь домены от мошеннической регистрации, кроме ручной проверки?

Существует также вопрос о скорости обнаружения от делегирования до минимизации последствий. Является ли это корректным измерением? Я хочу сказать, что в большинстве исследований используются общедоступные данные об объемах злоупотреблений DNS. И не поймите меня неправильно, эти объемы значительны, и все они шокируют. Но я бы сказал, что самая большая проблема злоупотребления DNS и, в частности, фишинга заключается в том, что все зависит от того, увидят ли это люди, станут ли они жертвами или потенциальными жертвами и сообщат ли они об этом.

Так что сейчас в большинстве отчетов, которые готовятся по этой теме, мы смотрим на зарегистрированный вред. Сколько из вас в зале получали фишинг или смиш на свой телефон или электронную почту, посмотрели на него, сказали: на этот раз я не попался, и удалили его? Если кто-то в этом зале не сделал этого и всегда сообщает о таких случаях, я вас хвалю. Но я не жду поднятия рук. О значительном количестве таких случаев не сообщается. А если о них не сообщается, то отрасль не в состоянии их предотвратить.

Так что изменение методологии регистрации - это потенциальное решение или путь, по которому следует идти, а также улучшение возможностей для обнаружения, чтобы их можно было быстро уничтожить, так чтобы домен активировался на шесть-семь секунд, был пойман и уничтожен, а не работал два дня, кто-то сообщил о нем, потребовалось два дня для проверки, и он был удален.

Сколько жертв было за этот четырехдневный период по сравнению с тем, если мы сможем улучшить обнаружение и уничтожать их гораздо быстрее? И, честно говоря, еще один момент для измерения, и это то, что очень сложно измерить, я не буду это выкидывать, мы уже должны это делать, но количество жертв на домен, потому что у вас может быть сотня жертв за секунду для хорошо сделанного фиша.

Таким образом, не обязательно количество доменов, используемых для фишинга, а количество жертв, которые на него попадаются, что позволяет оценить масштаб проблемы, потому что мы уже знаем, что даже на вершине айсберга, о котором мы говорим, который является общедоступным источником информации о фишинге, используются миллионы и миллионы доменов, и мы все можем признать, что есть еще много других, о которых не сообщается, так что мы их не видим, но мы также не смотрим на истинное воздействие, сколько жертв на каждого, и как это действительно влияет в финансовом плане на жителей планеты.

Я привел их в качестве дополнительных аргументов и тезисов для обсуждения, потому что отчет INFERMAL дал нам хорошее подтверждение того, что, да, мы всегда знали, что низкие цены стимулируют этот тип бизнеса, мы знали, что плохая проверка и верификация ваших владельцев доменов стимулирует этот трафик. Эхо добавлено для эффекта. Но теперь, как нам сделать следующие шаги? Как мы можем улучшить ситуацию? Что мы можем сделать, чтобы лучше измерить воздействие, а

также посмотреть, как мы можем лучше обнаружить, так чтобы мы могли более эффективно остановить эту проблему?

Потому что, смею предположить, даже если мы начнем взимать 1000 долларов за домен в год, то на самом деле мы лишим большинство людей по всей планете возможности зарегистрировать домен из-за его стоимости, но мы ничего не изменим для киберпреступников, которые собираются зарабатывать минимум 20 000 долларов за домен на тех убытках, которые они собираются нанести людям, так что они не будут возражать против такого увеличения стоимости. Это немного сократит их прибыль, так что нам придется искать другие решения. Спасибо.

NICOLAS CABALLERO

Спасибо, Джефф. Можем ли мы, хорошо, да, именно об этом я и говорил. Следующий слайд, да. Увеличение на 400%, я бы хотел обсудить это сейчас, и API - интерфейс программирования приложений, каково ваше мнение на этот счет? Действительно ли это проблема, что плохие парни имеют доступ к API, и, используя, не знаю, искусственный интеллект или что-то еще, они способны нанести ущерб и увеличить фишинговую активность? Действительно ли это так?

JEFF BEDSER

Нико, я ни на секунду не сомневаюсь, что массовая регистрация — это плохой способ приобретения крупных доменов для злоумышленных доменов. Однако метрика 400%, 401%, простите, один злоумышленник, регистрирующий DGA или домены алгоритмов генерации доменов для ботнета или кампании по распространению вредоносного ПО, может зарегистрировать 10 000 доменов за один раз, и это не сделает API плохим, потому что процент, основанный на API, может быть одним пользователем из всех пользователей, которые используют API. С другой стороны, следует ли сделать перерыв, если хотите, чтобы после того, как кто-то зарегистрирует 50 доменов, была сделана пауза, чтобы убедиться, что эти домены, которые регистрируются, выглядят так, как будто их собираются использовать для чего-то плохого, и есть много информации об инфраструктуре, которую можно использовать, чтобы посмотреть и убедиться, что они настроены для использования таким образом.

Так что, да, 10 000 доменов за раз - думаю, простой ответ: да, это не должно быть доступно, но сам API должен быть доступен, и проблема не в этом. Проблема в неограниченном доступе к API.

NICOLAS CABALLERO

Спасибо, Джефф. Позвольте мне открыть слово для комментариев или вопросов от членов GAC в зале или онлайн. Слово открыто, и я не вижу ни одной руки в зале. Простите,

простите, простите, да, есть две руки. У меня Индия и Австралия. Пожалуйста, Вам слово, Индия. Спасибо.

SUSHIL PAL

Спасибо, Джефф. Так что, я думаю, ясно, что верификация - это проблема, верно? Думаю, если у нас есть подтвержденные учетные данные регистраторов, вероятность злоупотребления DNS или значимости снижается, верно? И это также отражается в использовании, я думаю, алгоритма DGS, где проблема не в искусственном интеллекте. Это происходит потому, что непроверенные учетные данные через эти, ну вы понимаете, я имею в виду, что они передаются через массовые API, верно?

Так или иначе, я думаю, возможно, хотя проблема очень ясна, но все же мы обсуждаем с GNSO, как определить достоверность данных, каков их объем, потому что, если мы не заморозим эти вопросы достоверности данных WHOIS, я думаю, вы никогда не сможете перейти к аспекту проверки, верно? Так что, может ли GAC или SSAC, я думаю, вы, ребята, также можете убедить GNSO ускорить эти вещи? Я имею в виду, потому что иначе, знаете, мы все обсуждаем, мы все знаем о проблеме, но мы не делаем никакого значительного шага вперед, чтобы это сдержать.

JEFF BEDSER

Я не сказал во время презентации одну вещь, которую, вероятно, следует прояснить, — это то, что люди, с которыми мы боремся, люди, которые используют домены для этих целей, опережают нас на 10, а то и на 100 шагов. В последнее время наблюдается тенденция, когда легальные люди с легальными учетными данными создают аккаунт и медленно, в течение нескольких месяцев, накапливают портфель доменов, а затем просто продают этот портфель доменов с учетными данными преступнику, который затем использует эти домены в своих целях.

Несмотря на то, что более эффективные трения, связанные с более тщательной проверкой учетных данных, безусловно, полезны, я считаю, что полагаться на это как на решение проблематично. Другая реальная обеспокоенность заключается в том, что это публичное заседание, и я гарантирую, что люди, против которых мы здесь боремся, посмотрят эту запись и увидят, что мы знаем? Что мы уже знаем об их тактике и действиях, так чтобы они могли решить, какие следующие шаги они собираются предпринять.

Так что, если вы зададите вопрос о том, чтобы донести его до нужных групп, что будет дальше? Я считаю, что это относится к тому, что я говорил ранее, а именно, я думаю, что нужно вернуться к предыдущим пунктам, к предыдущему слайду, который гласил, что речь должна идти о лучшем обнаружении. Улучшение обнаружения и ускорение процессов устранения последствий — вот на чем нужно сосредоточиться, потому что

мы не собираемся устранять экономические стимулы для совершения краж у людей. Люди пытаются устранить экономические стимулы для совершения преступлений на протяжении всей истории человечества, и пока что в этом нет никакого успеха.

Преступность существует всегда, но если мы сможем придумать способ, как сделать так, чтобы тебя поймали, остановили до того, как ты успеешь причинить вред или хотя бы свести к минимуму число жертв, то стимулы к совершению преступления исчезнут, потому что появятся более выгодные преступления. Так что я не знаю, правильно ли это, что я говорю, пусть они занимаются другим видом преступлений, но смысл в том, что, конечно, если вы хотите улучшить обнаружение и минимизировать последствия, это действительно поможет решить эти проблемы.

SUSHIL PAL

Я имею в виду, не отменяя того, что лучшее обнаружение — это определенно, вы знаете, я имею в виду, что это конечная цель, я думаю, и когда я говорю о проверке, я не говорю, что это все и вся, но это первый шаг, верно? И я просто, я имею в виду, мы говорим и говорим, но мы не сделали эффективного шага, даже чтобы достичь чего-либо в процессе верификации на данный момент, особенно в gTLD, верно? У нас нет никаких проблем в ccTLD, которыми мы управляем.

Я думаю, что могу поделиться опытом своей страны, что, знаете, мы ввели двухфакторную верификацию, и количество злоумышленников значительно сократилось, значительно сократилось. Я бы хотел, чтобы то же самое можно было повторить. Это некоторые затраты, безусловно, для регистраторов, но это огромные затраты, которые мы платим из-за этих кибератак, которые никто из нас не осознает, потому что они не затрагивают, не ущемляют нас. Это ущемляет наших граждан, но, я имею в виду, тех, кого мы представляем, но для нас важно признать, что это первый шаг. Давайте сделаем первый шаг, не умаляя важности обнаружения и приобретения возможностей для их мониторинга.

NICOLAS CABALLERO

Спасибо большое. Индия, у меня Австралия, Европейская комиссия, Соединенное Королевство и Нидерланды. Так что, давайте перейдем к Вам, Австралия.

INGRAM NIBLOCK

Здравствуйте, Инграм Ниблок (Ingram Niblock) из Австралии. Мне просто интересно, каковы дальнейшие шаги в отношении самого исследования INFERMAL. Есть очевидное ограничение, описанное в отчете, что это не то, что делали преступники. Это просто особенности регистратора, который они изучали. Но мне интересно, предпринимались ли какие-либо усилия, чтобы, я полагаю, подтвердить гипотезы с регистраторами и

фактически пойти и сказать, поскольку у вас есть определенные домены, которые у них в блок-листе, и которые они использовали для исследования, что они сделали, как в масштабе, чтобы получить некоторые полезные данные, например, что люди, совершающие злоупотребления в этих конкретных случаях, действительно использовали на основе данных, которые, предположительно, есть у регистратора. Так ли это, да, я просто хотел узнать о дальнейших шагах в рамках самого исследования.

JEFF BEDSER Да, по этим вопросам мне придется отослать вас к офису технического директора, поскольку я знаю авторов отчета и их дальнейшие действия. В лучшем случае я могу дать вам информацию из разговоров. Вероятно, это не самый подходящий ответ. Так что, да.

NICOLAS CABALLERO Спасибо, Австралия. Европейская комиссия?

GEMMA CAROLILLO Спасибо большое, Нико. Гемма Каролилло (Gemma Carolillo) от Европейской комиссии. Моя коллега Мартина Барберо (Martina Barbero) является ведущей по темам злоупотребления DNS, она уже упоминала об этом в чате. Итак, у нас будет презентация отчета на заседании по злоупотреблениям DNS, в котором также примет участие OCTO, так что мы можем просто

переадресовать некоторые вопросы им. Но у меня есть два вопроса.

Один, более общий: поскольку этот отчет INFERMAL получил много откликов, и мы слышим некоторые ваши замечания по некоторым аспектам, есть ли у вас какие-то комментарии к отчету, к которым мы могли бы получить доступ и посмотреть, в чем конкретно заключаются нарушения или определенные моменты отчета, потому что это также помогло бы нам в чтении документа. И во-вторых, я понимаю, что, конечно, API не является проблемой как таковой, но это касается всего, что связано с технологиями. Так что, поскольку массовая регистрация представляется проблемой, какой вывод мы можем сделать из того, что должны быть ограничения на использование API, но возможно ли, что мы рассмотрим как практику в отношении массовых регистраций встречи лицом к лицу? Спасибо.

JEFF BEDSER

Итак, ответ на первую часть: нет, эти тезисы и комментарии не являются результатом консенсусного документа SSAC на данный момент, хотя мы можем, по сути, вернуть их руководству, чтобы посмотреть, сможем ли мы достичь консенсуса по заявлению о документе, который мы можем прочитать по INFERMAL, и какими, по нашему мнению, должны быть следующие шаги, это определенно кажется чем-то

заслуживающим внимания. Простите, второй вопрос уже вылетел у меня из головы.

Лично я думаю, что могу представить себе возможности, когда корпорация создает новый бренд или новую идентичность компании, и им может потребоваться зарегистрировать эту идентичность во многих TLD, и это может быть 2 000 регистраций одновременно, что эти инструменты могли бы быть оправданной целью в таком случае. Но мне трудно представить, чтобы что-то большее, чем это, было разумным объемом для массовых регистраций. Но, возможно, существуют бизнес-кейсы, о которых я не знаю. Но я думаю, что, например, по мнению джентльмена из Индии перед тем, как вы поставите..., хорошо, я воспользуюсь этим, существуют правила получения прав на вождение мотоцикла.

Существуют правила получения прав на управление автомобилем и другие правила на управление полугрузовиком. Вы должны получить разные лицензии в зависимости от вашей способности причинить вред другим людям, неправильно управляя этим транспортным средством. Если это транспортное средство должно быть использовано и доступно для людей, то я бы рассматривал API как инструмент, который больше похож на полугрузовик или поезд, где вам придется пройти более тщательную проверку того, кто вы и каковы ваши бизнес-цели, прежде чем вы получите к нему доступ. Тогда это не проблема инструмента, а проблема того,

кто имеет лицензию на использование этого типа инструмента.

NICOLAS CABALLERO Спасибо большое. У меня следующая Великобритания.

NIGEL HICKSON Извините, Найджел Хиксон (Nigel Hickson), Великобритания. Было невероятно интересно представить этот важный отчет в контексте, и спасибо SSAC за то, что он его рассмотрел. Мы всегда знали, что вы это сделаете. Я просто хотел бы узнать, возможно, я понимаю, что сейчас еще рано, но может ли это стать в результате ваших обсуждений какой-то рекомендацией или чем-то еще, учитывая важность тех рекомендаций, которые вы время от времени выпускаете. Спасибо.

RAM MOHAN Спасибо, Найджел. Мы еще не дошли до этого момента, чтобы определить или решить, должны ли мы давать рекомендации по этому вопросу. OCTO уже выступал перед SSAC с докладом на эту тему. Но мы не рассматривали этот вопрос и не говорили, есть ли в нем что-то дополнительное? Отчасти это связано с тем, что часть работы, которая может потребоваться здесь, скорее относится к разработке политики ICANN, чем к техническим рекомендациям ICANN.

В отчете INFERMAL содержится довольно много технических рекомендаций. Но это только мои мысли, мы не проводили конкретного обсуждения в рамках SSAC. Но спасибо за предложение, и мы поднимем этот вопрос на следующей беседе внутри SSAC, чтобы узнать, каково настроение его членов.

NICOLAS CABALLERO Спасибо. Рам, следующие у меня Нидерланды. Спасибо.

MARCO HOGEWONING Снова Нидерланды. Марко для протокола. Рам, вы сделали отличное замечание. Я действительно считаю, что в плане борьбы с проблемой это в основном проблема политики. Тем не менее, я также слышал, как Джефф говорил об улучшении обнаружения и совершенствовании, например, API. Так что мне интересно, есть ли место, помимо обсуждения политики, например, для улучшения технических стандартов по обнаружению или поведению API, чтобы решить часть этой проблемы? Есть ли место для технических решений?

RAM MOHAN Спасибо. Я вкратце расскажу об этом, и Джефф, возможно, вы тоже присоединитесь. Я не знаю, есть ли техническое решение, но я думаю, что здесь есть образовательный компонент. Когда вас пытаются обмануть, когда вас пытаются

разбить, знаете ли вы, что делать? Вы не только знаете, как обнаружить это, но и знаете, как сообщить об этом?

Потому что одна из проблем на данный момент, особенно в нашем сообществе, заключается в том, что если об этом не сообщается, то у вас нет достаточного количества данных, чтобы сказать, что было 1000 случаев, о которых было сообщено, еще 1000 случаев, на 10 % из них не отреагировали определенным образом, а затем давайте посмотрим на эти 10 % или любой другой процент, давайте посмотрим, кто стоит за этим, и увидим, каковы закономерности, чтобы попытаться понять, каким может быть поведение и характеристики в нашей экосистеме.

Так что практическая задача состоит в том, чтобы создать мощную образовательную кампанию, в которой будет сказано: сообщайте о злоупотреблениях, сообщайте о фишинге, сообщайте об этих проблемах. Затем, когда это будет сделано, давайте отследим, что происходит после этого. Тогда мы сможем получить данные, которые позволят сфокусироваться на том, где могут быть проблемные места или кто может способствовать возникновению проблем.

Сейчас мы, как мне кажется, находимся в режиме, когда часто пытаемся применить к этому широкий подход и сказать: давайте создадим новую политику, которая будет применяться ко всем, или нарисуем всю определенную группу участников в определенном свете, в то время как внутри этой

группы могут быть участники, которые делают блестящую работу, и другие, которые делают ее ужасно.

И наше внимание, я думаю, должно быть сосредоточено на тех, кто не соответствует требованиям. И как только у нас появятся эти данные, мы сможем сказать: вот лучшие практики, вот нормы, которых следует придерживаться, верно? И я думаю, что лучшие практики можно применять и без разработки политики, потому что тогда вы говорите, что это просто очевидно хорошо для лучшей гигиены, для лучшей экосистемы. Добавить нечего.

NICOLAS CABALLERO Спасибо. Рам, у меня Доминиканская Республика.

AMPARO ARANGO Это важная дискуссия. Выступает представитель Доминиканской Республики. Это очень техническая тема, но я думаю, что это суть того, с чем мы сталкиваемся сегодня в наших странах. И я бы хотела, как правительство маленькой страны, каковой мы являемся, а это Доминиканская Республика, вы в конце упомянули о том, что мы должны подать в суд, что мы должны сделать как правительство.

Во-первых, мы должны знать, какова ситуация в наших странах, в наших собственных администраторах доменов, операторах. Я представляю телекоммуникационный регулятор, наших операторов, все наши центры

кибербезопасности, наши центры реагирования на атаки, потому что за последние несколько лет Коста-Рика, например, два года назад пережила неприятную ситуацию, которая стоила им миллионы и миллионы долларов, и нарушила их систему здравоохранения.

Так что, с точки зрения правительства, и, возможно, от вашего имени, вы не можете сказать это так четко, но я думаю, что нам нужны стратегии. Какая-то четкая ориентация в отношении того, как продвигать DNSSEC в наших странах. Сколько людей знают об этом, будь то наши операторы, наши центры безопасности, наши собственные регистратуры. Я не знаю, есть ли это в моей стране или нет. Но как мы можем решить эту проблему отсутствия безопасности и кибербезопасности, которая является для нас чем-то большим? Я бы хотела услышать от вас, возможно, какие-то рекомендации, но я думаю, что они должны быть от SSAC и от GAC, потому что в долгосрочной перспективе это должно быть превращено в конкретные инструменты, потому что это связано с образованием.

Очень дорого иметь национальную стратегию, так чтобы мы могли регулировать все наши системы в рамках DNSSEC. Я не знаю, можете ли вы ответить на этот вопрос, но это действительно расстраивает. И я думаю, что у нас есть инструменты, так чтобы мы могли хотя бы смягчить последствия. Спасибо.

RAM MOHAN

Один из вызовов, с которым мы сталкиваемся в SSAC, заключается в том, что мы можем предоставить большое количество технических знаний и технической информации. Но мы не до конца понимаем, каковы ваши потребности, и на каком уровне вам нужна информация, верно? Так что, я думаю, нам нужно сотрудничать, чтобы понять, какого рода информацию вы хотели бы получить от нас.

Одна из вещей, которую мы начали делать, заключается в том, что раньше мы выполняли работу, а затем публиковали отчеты, очень технические отчеты объемом от 10 до 40 страниц. А теперь мы начали перерабатывать эти отчеты в резюме объемом 500 000 слов, которые представляют собой, если хотите, краткое изложение сути того, что мы пытаемся сказать в этих документах. Но это по-прежнему сосредоточено на наших исследовательских областях, на тех вещах, которые мы считаем важными потребностями.

Так что я призываю вас, и вас, в частности, прийти и поговорить с нами. Мы будем рады работать с вами напрямую. Но GAC в целом, пожалуйста, работайте вместе с нами, чтобы дать нам ясность по двум вопросам. Во-первых, какие виды информации будут полезны для вас. И, во-вторых, какой уровень информации вы хотите получить, какой уровень технической детализации вы хотите. Потому что по умолчанию мы начинаем с очень глубокого технического уровня. Это то, в чем мы хороши. Но если вы хотите, чтобы мы

поднялись на уровень или пару уровней выше, поговорите с нами, и мы вам поможем.

NICOLAS CABALLERO Спасибо большое. Ампаро, это предыдущий запрос на выступление? Хорошо. Нам пора заканчивать. У нас осталась одна минута. Последние вопросы или комментарии от GAC? Япония. Вам слово, пожалуйста.

НЕИЗВЕСТНЫЙ ОРАТОР Спасибо большое за презентацию. Я думаю, что вы подчеркнули важность сбора данных о фишинге и некоторых злоупотреблениях DNS. Я думаю, что существуют различные виды злоупотребления DNS, не только по определению ICANN, но и некоторые другие злоупотребления, такие как CSAM и, возможно, нарушение авторских прав, как в Японии, пиратство манги является очень большой проблемой и очень большим экономическим ростом. Я думаю, что корни проблемы схожи, и я считаю, что необходимо собирать данные о различных видах злоупотреблений, и, возможно, есть возможность сотрудничать с правительством для сбора данных. Но что вы думаете об этом?

RAM MOHAN Я думаю, что это важная тема, и мы готовы встать рядом с вами, чтобы предоставить технические детали и рекомендации, которые могут помочь в сотрудничестве. Но я

думаю, что окончательное решение, вероятно, будет заключаться в сочетании правительственной части, технической части и части политики, а также в поиске способа объединить их в рамках этого форума.

NICOLAS CABALLERO Спасибо вам большое, Рам. Нам пора заканчивать. Спасибо за ваши вопросы. Это было замечательное заседание, Рам, как всегда. Очень приятно, что вы здесь. Хотя для некоторых людей эти беседы немного техничны, но мы стараемся донести суть. Вы делаете все возможное, чтобы, с одной стороны, дать нам некоторые хорошие рекомендации, а с другой - помочь нам бороться со злоумышленниками.

Так что еще раз спасибо. Спасибо вам большое. Спасибо, Расс. Спасибо. У вас великолепная команда, Рэм, и, надеюсь, мы сможем провести еще одно заседание в Праге. Спасибо вам большое. Аплодисменты нашим друзьям из SSAC. Спасибо большое. Заседание закрыто. Увидимся завтра в 9 утра на церемонии приветствия и вручения премии за выдающиеся заслуги перед сообществом ICANN. Спасибо вам большое. Прекрасного вечера.

[КОНЕЦ СТЕНОГРАММЫ]