ICANN69 | Виртуальное годовое общее собрание – Изменения в WHOIS согласно GDPR: влияние на конечных пользователей и общественную безопасность
Среда, 21 октября 2020 года – 10:30 – 12:00 по CEST

[Это заседание записывается.]

ОЗАН САХИН: Спасибо и добро пожаловать на пленарное заседание с темой «Изменения в WHOIS в соответствии с GDPR: влияние на конечных пользователей и общественную безопасность». Меня зовут Озан Сахин и на этом заседании я исполняю обязанности координатора удаленного участия. Обратите внимание, что заседание записывается, и мы соблюдаем Стандарты ожидаемого поведения ICANN.

Во время заседания будут зачитываться только вопросы и комментарии на английском языке, присланные в окно вопросов и ответов. Эта функция доступна на панели инструментов Zoom. Я зачитаю вопросы и комментарии вслух во время, отведенное модератором этого заседания.

На этом заседании осуществляется стенографирование и перевод в реальном времени. Чтобы вывести на экран стенограмму в реальном времени, нажмите кнопку субтитров на панели инструментов Zoom. Устный перевод на этом заседании будет охватывать арабский, китайский, английский, французский и

русский языки и будет выполняться с использованием Zoom и удаленной платформы синхронного перевода под управлением Congress Rental Network. Участникам рекомендуем загрузить приложение Congress Rental Network в соответствии с инструкциями в чате в Zoom или из документа со сведениями о конференции в пакете заседания на сайте.

Если вы хотите говорить, поднимите руку в комнате Zoom и, после того, как координатор конференции назовет ваше имя, наша команда технической поддержки включит звук вашего микрофона. Сообщите для протокола свое имя и язык выступления, если это не английский.

Во время выступления обязательно отключите микрофоны на всех остальных устройствах, включая приложение Congress Rental Network. Кроме того, говорите четко и в умеренном темпе, чтобы обеспечить точность перевода.

Хочу отметить, что удаленные участники не могут нажимать кнопку микрофона и включать собственный звук во время этого заседания, не прибегая к помощи группы технической поддержки.

Все участники заседания могут оставлять в чате комментарии. Для этого выберите пункт «ответить всем докладчикам и участникам» в раскрывающемся меню раздела чата. После этого все смогут увидеть ваш комментарий.

Обратите внимание, что личная переписка возможна только между докладчиками в формате вебинара Zoom, и сообщение, отправленное докладчиком или обычным участником, также будет видно организаторам сеанса, соведущим и другим докладчикам.

А теперь я передаю слово Джонатану Зуку.

ДЖОНАТАН ЗУК: Спасибо. Говорит Джонатан Зук, заместитель председателя консультативного комитета At-Large. Как многие из вас знают, At-Large рассматривает неправильное использование DNS и другие связанные с этим вопросы как своего рода проблему кампании на протяжении года, но я чувствую, что многие из этих разговоров были отчасти повторяющимися и не дали каких-то конкретных результатов. И во многом это результат недостатка данных. Просто со всех сторон много риторики, что очень затрудняет рациональный разговор на эти темы.

И мы часто видели в контексте ICANN, что иногда прогнозы, сделанные в пылу страсти по поводу новой политики, не сбываются; что имеет место какой-то другой исход. Например, когда впервые предлагалась программа новых gTLD, Sony предложила на слушаниях по проверке полномочий инвестировать 12 миллионов долларов в защитные регистрации, но в конечном счете они этого не сделали. В итоге

они нашли другой способ защиты своего товарного знака в этих новых gTLD.

Точно так же с внедрением GDPR и последующим тревожным звонком сообщества ICANN – возникла схватка, верно? Это привело к внедрению временной спецификации, формированию рабочей группы ускоренного PDP по вопросу о том, как ICANN будет соблюдать правила GDPR. В результате произошли кардинальные изменения в данных, которые общедоступны через систему WHOIS, и была введена система нового типа, в которой людям нужно было запрашивать информацию у сторон, связанных договорными обязательствами.

И поэтому в ходе процесса EPDP, к лучшему или к худшему, были своего рода менеджеры данных и стороны, запрашивающие данные, которые стали этими двумя важными сторонами в этих обсуждениях.

Итак, идея этого пленарного заседания состоит в том, чтобы собрать эти стороны вместе и обсудить, что на самом деле происходит в этот промежуточный период. Другими словами, на каком уровне выполняются запросы данных и как они обрабатываются. Кажется, нас часто удивляет, что цифры меньше, чем мы думаем; что было не так много запросов или не так много жалоб на соблюдение условий контракта и так далее. И поэтому кажется, что начинать с базовых фактов

лучше, поскольку мы пытаемся обсудить данные владельцев доменов и их использование.

Вполне возможно, что стороны, которые в первую очередь были озабочены доступом к данным о владельцах доменов, нашли альтернативные способы получения этой информации для защиты прав на товарные знаки, обеспечения правопорядка и защиты потребителей. И поэтому они пытаются достичь того уровня, на котором мы находимся сейчас, пару лет спустя, с точки зрения этих данных, потребности в них, их доступности, эффективности, с которой они могут быть получены запрашивающими сторонами от сторон, связанных договорными обязательствами, и т. д. Именно это мы надеемся обсудить в рамках этого пленарного заседания, на самом деле это просто миссия по установлению фактов о том, как обстоят дела сегодня, каков статус-кво.

Так что, надеюсь, мы постараемся свести к минимуму идеологические дискуссии и по-настоящему максимизировать обсуждение данных и фактов о том, как выглядит статус-кво.

Чтобы начать разговор, мы собираемся поговорить – узнаем некоторые точки зрения от одного из сообществ запрашивающих, а именно от правоохранительных органов и защиты потребителей. И с этой целью я дам десять минут Лорин Капин из FTC и Габриэлю Эндрюсу, чтобы они рассказали о перспективах правоохранительных органов, необходимости в

этих данных, альтернативных вариантах, которые представили сами, и о том, как выглядел процесс за последние пару лет.

На этом передаю слово Лорин.

Спасибо. Вам нужно включить микрофон.

ЛОРИН КАПИН: Для меня еще рано, так что особый привет всем, кто находится в непростом часовом поясе. И я уверена, что людям, которые не там, должны быть очень благодарны.

Меня зовут Лорин Капин, и я здесь, чтобы поделиться с вами точкой зрения конечного пользователя системы защиты прав потребителей на то, как общественность использует WHOIS.

Давайте перейдем к следующему слайду.

Я юрист в Федеральной торговой комиссии. Я работаю в Управлении по международным делам защиты прав потребителей и занимаюсь этими вопросами, как и мое агентство, в течение ряда лет. Но взгляды, которые вы сейчас услышите, они мои. Они не отражают официальную позицию Федеральной торговой комиссии, которая выражается через комиссаров. Итак, вы слышите меня, старшего юриста Федеральной торговой комиссии.

Следующий слайд, пожалуйста.

И я также сопредседатель Рабочей группы по общественной безопасности, которая уже довольно долгое время отстаивает эти вопросы.

Таким образом, у Федеральной торговой комиссии есть замечательный ресурс, где потребители и общественность не только в Соединенных Штатах, но и во всем мире могут подавать жалобы, если они стали жертвами или обеспокоены обманом, мошенничеством или жульничеством. И это называется нашей базой данных «Consumer Sentinel». Эта база данных получает сотни тысяч жалоб каждый год со всего мира.

Неудивительно, что когда мы смотрим на эти жалобы, мы можем получить небольшую фотографию того, как общественность, простые люди, пользователи, которые выходят в Интернет, чтобы покупать товары, встречаться с людьми, получать информацию, как общественность использует WHOIS, потому что ссылки на WHOIS в их жалобах верны.

Я изучила часть этих жалоб, в частности, после вступления в силу изменений в системе WHOIS. И когда я говорю «изменения», я имею в виду те изменения, которые скрывают определенную информацию, в частности контактную информацию владельца домена, ответственного лица. И вот что я нашла. Конечные пользователи используют WHOIS для различных целей. Но по сути они ищут признаки надежности. Они хотят просматривать записи WHOIS, чтобы выполнить

комплексную проверку, а также отслеживать подозрительные или злонамеренные действия. Они хотят выяснить, кто виноват. Иногда они хотят попытаться связаться с ними. И иногда я знаю, читая эти жалобы, что они расследуют что-то связанное с жульническими действиями, то есть они разговаривают по телефону с кем-то, пытаясь выяснить, обманывают их или нет. И они идут к своему компьютеру и смотрят на домен, который, возможно, привел их к этому телефонному звонку.

Потребители отметили после этих изменений в WHOIS, что в записи скрыта или отсутствует информация. И из-за отсутствия информации они могут предположить, что бизнес нечестный. И это предположение может быть верным, а может и нет. И, кстати, эти жалобы поступают в FTC. Они не проверяют жалобы. Они просто получают их и используют как элемент данных.

Итак, пользователи отмечали, что детали могут быть скрыты, и это мешает их комплексной проверке. Например, один человек пожаловался на отсутствие данных по коммунальному предприятию. Итак, из этого облака слов вы можете увидеть, как разные люди используют это, и эти термины я нашла в жалобе... в жалобах, которые я рассмотрела.

Чтобы дать вам представление, потому что мы стараемся быть лаконичными и у нас осталось совсем немного времени. Но чтобы дать вам представление – пожалуйста, следующий

слайд – о типах мошенничества, для расследования которых люди используют WHOIS: Поддельные товары, романтические аферы, аферы с домашними питомцами. Вы будете удивлены, узнав, сколько существует афер с домашними питомцами!

Следующий слайд, пожалуйста.

Мошенничества с изобретениями, фишинг. А в эпоху COVID у нас также есть фишинговые атаки, связанные с коронавирусом. Мошенничество с техподдержкой, мошенничество от имени госучреждений, фальшивые чеки, мошенничество с вакансиями и многое другое.

Я также хочу подчеркнуть, что люди не просто используют контактную информацию в записи WHOIS. И в этом смысле людям повезло, потому что там все еще есть некоторая полезная информация, например, когда домен был создан и где он был создан. Так что это всего лишь разновидность того, как конечный пользователь использует данные WHOIS для базовой самозащиты, и в этих жалобах отмечается некоторое разочарование по поводу того, что определенная информация для этой цели недоступна.

Я передаю эстафету своему коллеге Гейбу.

ГАБРИЭЛЬ ЭНДРЮС: Ладно. Итак, следующий слайд, пожалуйста.

Когда я говорю, я говорю от имени правоохранительных органов. И я отмечаю, что, несмотря на просьбу о предоставлении данных, чрезвычайно сложно получить точные цифры от правоохранительных органов о том, когда их нервирует несовершенный доступ к WHOIS.

Кроме того, правоохранительные органы склонны объединять несколько вопросов воедино. Они не всегда понимают, как лучше. Но будь то GDPR или Закон о конфиденциальности потребителей Калифорнии или услуги сохранения конфиденциальности и регистрации через доверенных лиц, в конце концов, все, что действительно имеет значение для полицейского, следователя или сотрудника службы общественной безопасности – это то, что они пытаются получить доступ к данным, а данных для них нет.

Итак, говорить об одной из этих проблем – значит говорить обо всех с точки зрения полицейского.

Следующий слайд, пожалуйста.

Я хотел бы подробнее рассказать, сколько времени требуется, чтобы получить доступ к данным. И это важно. Бывает разная продолжительность, разные временные рамки, в зависимости от обстоятельств.

Раньше вы могли выполнить поиск в общедоступных источниках и получить обратно информацию о владельце домена примерно за десять секунд, верно? К такому привыкли многие копы, основываясь на своем прошлом следственном опыте.

Если они не получат эти данные, они могут и, вероятно, даже не узнают, что могут обратиться к регистратору для получения доступа к полным данным, если они были отредактированы для целей GDPR. Если нет услуги сохранения конфиденциальности/регистрации через доверенных лиц, и они каким-то образом знают, что могут связаться с ними, ответы были разными. Некоторые регистраторы напрямую отвечают на запросы правоохранительных органов о предоставлении неотредактированной информации, и мы это ценим.

Некоторые отвечают только местным правоохранительным органам, имея в виду ту же страну, что и запрашиваемое агентство. И если вы не из той же страны, вам не повезло.

Некоторые потребуют судебного разбирательства.

Для удобства переводчиков, если вы слышите, как я говорю «судебное разбирательство», я имею в виду постановление суда, повестку с вызовом в суд или что-то в этом роде.

И сроки для них увеличиваются, как и следовало ожидать. Если регистратор отвечает добровольно, это может быть не десять

секунд, а часы, может быть, дни. Если речь заходит о судебном разбирательстве, то это в среднем от нескольких дней до двух недель – это то, что я ожидал бы для получения, обработки и получения ответа на судебное разбирательство.

Если вы находитесь в другой юрисдикции и вам требуется судебное разбирательство, вам, вероятно, не повезло. Но теоретически вы могли бы, если вы подписали Договор о взаимной правовой помощи, подать запрос MLAT и получить данные через шесть месяцев.

Следующий слайд, пожалуйста.

Поэтому, когда мы говорим о воздействии, я хотел бы выделить один из процессов, на которые мы оказали наибольшее влияние, – одну из наиболее затронутых обязанностей, а именно уведомление жертв. В приведенном здесь примере показан пример взлома деловой электронной почты, который является одним из самых распространенных видов мошенничества в Интернете на сегодняшний день. По оценкам, в 2019 году мы потеряли по этой схеме 23 миллиарда долларов. И число, похоже, удваивается с каждым годом. Не удивлюсь, если в этом году оно приблизится к 50 миллиардам.

В этом примере вы видите, что плохой парень выдает себя за генерального директора с доменом ceo@example.com, который он зарегистрировал. Это очень похожий домен, иногда

называемый гомоглифом, и он специально нацелен на жертву. Он отправляет электронное письмо с просьбой о банковском переводе. Вот как работают схемы. Если он добьется успеха, уйдут миллионы долларов. В прошлом мы, как следователи, выполняли обратный поиск в DNS этого владельца плохого домена и видели много других доменов, которые они зарегистрировали. И мы, вероятно, можем сделать вывод о большинстве настоящих жертв, потому что их домены похожи друг на друга, верно? Если мы сможем сделать это достаточно быстро, если мы сможем действовать очень быстро, мы сможем контролировать дальнейшие DNS-запросы к этим жертвам, определять для них контактную информацию и сообщать им в режиме реального времени, что они подвергаются активной атаке плохого парня.

Теперь, даже если это небольшая задержка в проведении этих поисков из-за того, что на протяжении этого процесса выполняется несколько поисков, вы отрицательно влияете на нашу способность проводить эти важные уведомления жертв до такой степени, что, я думаю, это больше не делается. Не потому, что мы не пытаемся, а потому, что самый первый шаг к получению данных обо всех этих дополнительных доменах потенциальных жертв требует юридического процесса, который теперь потребует дней или недель.

Мы все еще можем пробовать делать это. Я просто очень хотел подчеркнуть, что это одно из последствий в реальном мире, которое возникает даже из относительно незначительных задержек, от секунд до минут, дней и недель. Это имеет колоссальные последствия. И я вижу, что я укладываюсь по времени, и время драгоценно, поэтому я собираюсь передать слово следующему докладчику.

ДЖОНАТАН ЗУК: Спасибо, Габриэль. Сейчас мы собираемся послушать людей, занимающихся исследованием кибербезопасности. Грег Аарон и Лайман Чапин, давайте.

ГРЕГ ААРОН (GREG AARON): Привет, это Грег Аарон.

Следующий слайд, пожалуйста.

Лайман и я недавно провели небольшое исследование фишинга и попытались собрать информацию о том, сколько таких атак происходит, где это происходит и так далее.

(Нет звука)

В результате было получено почти 300 000 фишинговых URL-адресов, и они присутствовали в более чем 99 000 доменных именах. Затем мы выяснили, где они размещены. Мы

посмотрели время событий и выяснили, какие регистраторы, хостинг-провайдеры были задействованы.

Мы обнаружили, что фишинг на самом деле довольно концентрированный. Он имеет тенденцию группироваться в определенных TLD. У некоторых хостинг-провайдеров гораздо больше, чем у других. Если перейти к URL-адресам, вы можете увидеть результаты исследования.

Мы видим, что фишинговые домены используются быстро. Почти... большинство из них используются в течение 14 дней с момента создания домена, некоторые из них, многие из них – всего в течение трех дней с момента создания.

Мы также увидели, что фишинг – более серьезная проблема, чем сообщается. Каждый раз, когда вы добавляете новый источник данных, вы узнаете о новых фишинговых событиях, о которых другие не знали.

Существуют также приемы уклонения, которые используют преступники.

Поэтому, когда вы смотрите на эти данные, вы можете выяснить нижний предел проблемы, но вы не можете установить верхний предел того, что происходит.

Один из способов узнать объем фишинга – по тому, сколько атак зарегистрировано и заблокировано, и... пытаться найти

этот материал... мы находим, но иногда это сложно. Многие из этих источников перекрываются на очень небольшое количество. И мы также не наблюдаем фишинга в определенных частях света. Из-за отчетности явно не хватает данных о фишинге в таких странах, как Китай и Россия.

Таким образом, одним из факторов, влияющих на нашу способность обнаруживать фишинг, является отсутствие информации WHOIS. Есть две проблемы. Следующий слайд.

Конечно, когда вы пытаетесь выяснить, насколько велик элемент, это зависит от того, что и как вы измеряете. Google, например, интересен своими измерениями, потому что они действительно могут видеть, сколько фишинга они блокируют в браузере Chrome. Так что это очень интересная мера. Этот слайд взят из их программы Safe Browsing, а красным показано количество фишинговых сайтов, которые они блокировали. Это интересно, потому что у них есть единообразный метод, который они применяют в течение длительного периода времени.

Вы видите, что фишинг набирает обороты. В то же время сокращается вредоносное ПО. Этому можно найти объяснение. Количество киберпреступлений и их место со временем могут меняться. Одна из причин, по которой вредоносное ПО сокращается, заключается в том, что некоторые ботнеты были заблокированы. Это также связано с тем, что преступники

меньше заинтересованы в запуске некоторых видов банковского вредоносного ПО. Вместо этого они перешли к другим видам преступлений, включая мошенничество с взломом деловой электронной почты, которое только что описал Гейб.

Поэтому, когда вы хотите понять, сколько существует киберпреступлений, это зависит от того, что вы измеряете, как вы измеряете, и вам также нужно видеть общую картину. И если вы не измеряете некоторые вещи, вы просто не узнаете о них.

Следующий слайд, пожалуйста.

Итак, зачем нам нужна информация WHOIS? Нам нужна информация, потому что мы действительно хотим узнать о таких вещах, как время регистрации доменного имени, и регистраторы, у которых оно было зарегистрировано. Это не конфиденциальная информация. Как мы видели, дата регистрации действительно имеет значение.

Одна из проблем, с которыми мы сталкиваемся прямо сейчас – это ограничение частоты. Это означает, что операторы регистратуры и регистраторы разрешают вам делать определенное количество запросов в течение определенного периода времени. SSAC ICANN подготовил об этом документ. Он не позволяет нам получить неконфиденциальную

информацию, которая позволила бы нам увидеть и, возможно, обнаружить больше фишинговых атак.

Кроме того, люди, которые пытаются бороться с этой проблемой, смотрят или раньше смотрели на контактную информацию в регистрационной записи. И это было важно, потому что преступники очень часто, как вы понимаете, подделывают свои данные. Они не дают точной контактной информации. И это можно проверять, и если данные неточные, это показатель недобросовестности владельца домена.

Это также позволило нам увидеть, зарегистрировала ли определенная сторона более одного доменного имени, и вы можете выполнить поиск и сравнить информацию. После внедрения GDPR это уже не так полезно.

Но выводы нашего отчета подтвердили то, что мы знали уже давно, а именно: когда преступники регистрируют одно доменное имя, они очень часто регистрируют целую группу, и мы видим, что поймать эти группы тоже стало сложнее, чем прежде. В некоторых случаях мы можем видеть длинные последовательности доменных имен, и некоторые из них были обнаружены и занесены в черный список, но вы также можете увидеть, какие из них были пропущены.

Следующий слайд, пожалуйста.

Мы также обращаем внимание на продолжительность фишинг-атаки. Это действительно отличные данные, собранные людьми из PayPal, Google и университета штата Аризона. Это было действительно плодотворное исследование, проведенное в этом году. И у этих компаний есть отличная аналитика, потому что они могут видеть, на что люди кликают, и они могут отслеживать вещи от первого посещения определенного фишингового сайта до последних посещений, а затем, если это был фишинг с участием PayPal, они могли бы увидеть, как люди стали жертвами и многие из них потеряли деньги со своих счетов и так далее.

И эти данные хорошо согласуются с другими исследованиями, в том числе с некоторыми, которые я провел, но они показывают, что фишинговая атака непродолжительна.

С момента первого посещения и до момента, когда фишинг обнаруживается, проходит около восьми часов, а вся фишинговая атака обычно занимает около 17 или 18 часов. Таким образом, к тому времени, когда фишинговая атака обычно обнаруживается, большая часть ущерба уже нанесена. Большинство жертв пришло на сайт, и те, кому суждено потерять деньги на афере, уже стали жертвами.

Следующий слайд, пожалуйста.

Мы также обнаружили, что около 60% доменов, используемых для фишинговых атак, зарегистрированы фишерами.

Домены, используемые для фишинга, делятся на две категории. Во-первых, фишеры просто идут и покупают доменные имена, а затем используют их для запуска своих поддельных сайтов. Фишеры также могут использовать доменные имена, которые они взломали на хостинге, поэтому они фактически занимаются фишингом на чужое доменное имя, невиновной стороны.

Как реагирующая сторона, мы хотим, чтобы о таких сайтах позаботился провайдер хостинга, сохранил остальной контент и предотвратил любой побочный ущерб для невиновного владельца домена.

Однако доменные имена, зарегистрированные фишерами, могут быть просто приостановлены без какого-либо сопутствующего ущерба.

С помощью нашей методологии мы обнаружили, что около 60% доменных имен попадают в эту категорию злонамеренных регистраций.

Команда из SIDN Labs и AFNIC – это операторы регистратур .NL и .FR – создала отдельную систему. Их методики немного пересекались. Они создали очень сложную систему, и они нашли 57%. Таким образом, мы были довольно близки по процентному соотношению, и они проделали очень хорошую работу, которая, на мой взгляд, была очень интересной.

Итак, следующий слайд. Я думаю, что некоторые выводы таковы. Мы обнаруживаем множество злонамеренных регистраций, и сейчас делать это стало сложнее. Одна из причин заключается в том, что у нас нет некоторых данных, которые были доступны ранее, и это своего рода очевидный вывод.

В некотором смысле контактные данные – это то, что отличает одно доменное имя от другого. Это показатель недобросовестности. Очевидно, что информация о том, кто это зарегистрировал или кто якобы зарегистрировал, безусловно, очень важна.

Хорошая новость, если таковая имеется, заключается в том, что регистраторы и операторы регистратур все еще имеют доступ к этим данным. Они видят это даже тогда, когда никто другой не видит.

А поскольку большая часть фишинга совершается самими фишерами, которые регистрируют эти доменные имена, у регистраторов и операторов регистратур есть возможность продолжать использовать эти данные. Однако мы видим постоянный фишинг в определенных TLD и у определенных регистраторов.

Что касается EPDP, одним из результатов было то, что у нас будет целевое время обработки запросов на данные. Запросы, связанные с кибербезопасностью, с фишингом, предусмотрены

в самом GDPR. Это называется законными интересами для запроса данных.

Однако этот пятидневный цикл, а затем, возможно, дойдет до десяти дней, будет в целом неэффективным, потому что фишинговые атаки, все меньше, меньше – длятся меньше суток.

Таким образом, данные через систему SSAD могут поступать быстро или медленно, а медленные запросы не помогут решить непосредственную проблему.

Так что фишинг, безусловно, является отличным кандидатом для проверки автоматизации. Это то, на что группа внедрения должна будет обратить внимание. Но если это можно сделать, система SSAD действительно сможет предоставить некоторые полезные данные для реагирования на фишинг и снижения уровня виктимизации.

Спасибо.

ДЖОНАТАН ЗУК: Спасибо, Грег.

Думаю, Марк пока еще не подключился. Я прав?

>> Правильно.

ДЖОНАТАН ЗУК: Ладно. Затем я хотел бы двигаться дальше и передать слово Милтону, чтобы мы могли приступить к обсуждению, потому что, очевидно, идет довольно оживленная дискуссия. Итак, давайте пройдемся по этим исходным презентациям и начнем разговор.

Милтон, пожалуйста, вам слово.

МИЛТОН МЮЛЛЕР: Приветствую всех. Я Милтон Мюллер. Я профессор Технологического института Джорджии в США. И, кстати, все в этой группе из Соединенных Штатов. Разве это не интересно?

Фактически, дебаты о WHOIS были сосредоточены на разногласиях между Европой и США в отношении закона о конфиденциальности.

Давайте перейдем к следующему слайду.

Кое-что, о чем вы еще не слышали – это то, почему я нахожусь в этой группе, и я на самом деле говорю о правах и интересах владельца домена, человека, который регистрирует доменное имя. Не слишком сложно понять, почему люди, регистрирующие домены, заинтересованы в сокрытии определенной личной информации, конфиденциальной личной информации. Согласно многим законам о конфиденциальности,

они действительно имеют законное право, а также заинтересованы в защите этих данных.

Фактически, наша собственная Федеральная торговая комиссия, в которой работает Лорин, имеет много информации о том, как не следует делать такую информацию, как ваш адрес электронной почты, и другую личную информацию, такую как ваш номер телефона, легко доступной в Интернете, где ее может скопировать и использовать кто угодно. И, конечно же, все, что мы действительно сделали с применением GDPR к WHOIS – это использовали общее разумное представление о том, что преступники и злоумышленники могут злоупотреблять открытой PII. И, как правило, не рекомендуется делать свою электронную почту и физический адрес доступными случайным образом для всех и каждого в Интернете.

Несмотря на это, в существующем WHOIS, конечно, все еще довольно много информации: там все еще будут имя владельца домена, страна, а в некоторых случаях даже штат и город. Надеемся, что мы создали новые эффективные методы для более быстрого раскрытия скрытых данных.

Мне любопытно, почему At-Large больше не интересовался правами владельца доменного имени. Я знаю, что они должны представлять пользователей. И я хотел бы знать, какова позиция европейских структур At-Large по WHOIS. Потому что

мы, конечно, не слышали никакой поддержки в отношении GDPR от ALAC во время процесса EPDP.

Следующий слайд, пожалуйста.

Мне очень понравилось вступительное слово Джонатана перед группой, можем ли мы попытаться поговорить здесь о фактах. Так что получить окончательную информацию о том, что произошло, непросто. Но мы помним – мы не говорим о том, вреден ли фишинг или как он работает, мы говорим о том, как эти вещи работают до и после скрытия данных из-за нашего соответствия требованиям GDPR.

Итак, если вы посмотрите статистику Google, которую показывал Грег, за период с 15 декабря по май 2018 года, что является периодом... по сути, 17-месячным периодом до того, как сокрытие вступило в силу, и вы посмотрите на 18-месячный или 17-месячный период после его внедрения, в отношении сайтов с вредоносным ПО, вы увидите спад до и после. Хотя после этого спад был явно более значительным.

И если вы посмотрите на фишинговые сайты, вы увидите очень большой рост как до, так и после применения сокрытия.

Я также просмотрел некоторые данные о спаме, хотя очень сложно найти данные о спаме за длительный период. И, опять же, вы не увидите никакой связи между сокрытием данных в 2018 году и размером и масштабом проблемы. Установить

какую-либо статистическую корреляцию между сокрытием и изменениями в проблеме просто невозможно.

Я думаю, что аргумент, который вы бы представили на основе данных о связи между сокрытием и нашими проблемами с киберпреступностью, является чрезвычайно слабым.

Это не потому, что в некоторых случаях правоохранительным агентствам нецелесообразно иметь быстрый доступ к этим данным. Очевидно, что он им нужен. Это также факт, что быстрый доступ является вектором угрозы, частью причины проблемы. И остается фактом, что все больше и больше фишинга и все больше и больше злонамеренных регистраций, преступники научились подделывать информацию, и они придумали очень умные способы перекрестных ссылок и получения ложной информации о личности, и людям, просматривающим данные WHOIS, выявить это очень непросто.

В заключение по этой проблеме фишинга позвольте сказать, что когда я преподаю кибербезопасность студентам Технологического института Джорджии, мы выполняем упражнение, в котором команды из пяти студентов разрабатывают фишинговое электронное письмо и отправляют его своим инструкторам и проверяют, смогут ли они их обмануть. Студенты обнаружили, что фишинговые домены часто обнаруживаются различными алгоритмами среди хостинговых компаний, среди интернет-пользователей,

производителей браузеров, которые используют такие показатели, как скорость регистрации, насколько домен новый и соответствует ли он определенным строкам. И, возможно, около половины этих студентов обнаруживают, что они... их фишинговый домен заблокирован еще до того, как они успевают выполнить задание и отправить его мне.

Следующий слайд, пожалуйста.

Повторю, мы не закрыли доступ к этой информации полностью. В рамках нового процесса политики мы внедрили централизованный и стандартизированный метод подачи запросов на раскрытие информации. И я думаю, мы должны понять, и мы не можем игнорировать это, что все дело в соответствии требованиям. Это не является необязательным; так, ребята? Мы должны соблюдать закон. Благодаря кропотливым усилиям в рамках EPDP мы разработали механизм раскрытия информации, соответствующий GDPR, что означает, что многие запросы просто необходимо рассматривать, чтобы убедиться в наличии законного интереса и законности подателя запроса, и так далее.

Я закончу на этом и с нетерпением жду активного обсуждения с другими участниками дискуссии и с аудиторией.

Спасибо за то, что выслушали меня.

ДЖОНАТАН ЗУК: Большое спасибо, Милтон. Это снова Джонатан Зук, для протокола. И я хочу повторить кое-что из сказанного Милтоном: это произошло, и это имело отношение к соблюдению закона. И поэтому, когда мы начнем обсуждать это, я думаю, что мы хотим посмотреть, как выглядит мир в соответствии с этим законом, не переосмысливая, был ли закон хорош или что-то в этом роде, а вместо этого, что за поток данных был между подателями запросов и хранителями данных. Смысл в этом. Не для того, чтобы снова вести тот же разговор, что и EPDP в течение двух лет, а просто для того, чтобы оглянуться назад на то, каким был процесс с тех пор и как выглядят эти отношения.

Я думаю, что Оуэн будет идеальным вариантом для выступления по этому вопросу. Они только что составили отчет о последних запросах данных. Не помню, как давно это было. Есть вебинар, который стоит посетить. Я уверен, что Оуэн укажет нам на это и расскажет немного об этом здесь, и немного расскажет о том, как это выглядело со стороны хранения данных в уравнении с момента реализации временной спецификации, и как выглядели последние пара лет.

Пожалуйста, Оуэн.

ОУЭН СМИГЕЛЬСКИ: Спасибо, Джонатан.

Давайте подумаем. Я вижу, что видео включено, но я не виден на экране, или люди могут меня видеть?

ОЗАН САХИН: Привет, Оуэн. Да, мы вас видим.

ДЖОНАТАН ЗУК: Да, мы вас видим и слышим.

ОУЭН СМИГЕЛЬСКИ: Что ж, превосходно. Привык смотреть сам, но не... Хорошо. Следующий слайд.

Итак, я Оуэн Смигельски. Я представляю регистратора Namecheap. Я также заместитель председателя группы заинтересованных сторон-регистраторов по вопросам политики. И материал, который я собираюсь вам представить – это сокращенная версия вебинара, который регистратуры и регистраторы провели в сентябре. Есть ссылка на вебинар, презентацию, а также на записи в календаре GNSO. И я поместил ссылку на слайды здесь, чтобы все могли это увидеть и пойти посмотреть. Поэтому я приглашаю вас взглянуть на это, потому что там гораздо больше информации.

Я участвовал в том вебинаре вместе с тремя коллегами, собравшими информацию, которую я сейчас собираюсь представить: Алан Вудс из регистратуры Donuts, Бет Бэкон, PIR, оператор домена .org, и Сара Уайлд из регистратора Tucows. Так что я должен поблагодарить их за большую часть материала, который я собираюсь здесь представить.

Следующий слайд, пожалуйста.

Я думаю, что во многих этих обсуждениях упускается то, что GDPR и защита данных не являются чем-то новым. Корни этого восходят к концу Второй мировой войны, и беспокойство, которое существовало в тот период, было вызвано тем, что личная информация людей использовалась для профилирования и таргетирования многочисленных групп со стороны штатов и других субъектов. Это включало имена, религию, этическое происхождение, сексуальную ориентацию и другие факторы. И поэтому после ужасов того времени интерес к конфиденциальности в защите персональных данных приобрел очень большое значение, и это продолжается до сих пор. Вот почему защита данных субъектов данных является такой важной проблемой и почему это просто нельзя упускать из виду, потому что некоторые люди считают, что им иногда доставляют неудобства. И это было включено во Всеобщую декларацию прав человека в 1948 году. Было заключено еще несколько договоров и соглашений, и первый

в мире национальный закон о защите данных был принят в Швеции в 1973 году, а до создания ICANN в 1998 году их появилось еще несколько.

Следующий слайд, пожалуйста.

Итак, есть семь принципов, которые присутствуют во всех европейских законах о защите данных, и все они касаются защиты субъекта данных, а не обязательно третьих лиц. Так что я не буду здесь их рассматривать, но некоторые из них нужны, чтобы ограничить цель для сбора этой информации. Вам не нужно получать больше данных, чем необходимо. Вам нужно следить за тем, чтобы они хранились определенный период времени. Это нужно делать безопасным способом. И должна быть подотчетность по этим данным.

До вступления в силу GDPR неограниченный доступ к регистрационным данным через WHOIS нарушал многие из этих принципов.

Следующий слайд, пожалуйста.

Так что это всего лишь несколько основных моментов или вопросов. GDPR не новость. В него были внесены некоторые незначительные изменения, чтобы повысить ответственность, но то, что было предусмотрено GDPR, существовало в Европе, а также в других странах и договорах на десятилетия раньше.

WHOIS никогда не отключалась. Она и сейчас на месте. Это просто соответствует закону. И я знаю, на этом вебинаре уже несколько раз повторялось, что данные WHOIS необходимы для прекращения сообщений. Это не лучший способ сделать это. Лучший способ – сообщить об этом стороне, связанной договорными обязательствами, либо регистратору, либо регистратуре, либо напрямую поставщику услуг хостинга. Это те, кто может позаботиться об этом. После этого можно провести анализ, чтобы увидеть, кто что делал и как это предотвратить, а затем это можно будет сделать после того, как закончится ограниченное время для остановки фишинговой атаки.

Отчеты и презентации не помогают решить проблему. Нам необходимо получать сообщения об этом, чтобы мы могли принять меры.

Все эти законы о защите данных, включая CCPA в Калифорнии, закон о конфиденциальности в Бразилии, и в других штатах, которые продолжают появляться, предоставляются права субъектам данных. Это не дает права третьей стороне получать доступ к этим данным и не создает обязательств по раскрытию этих данных.

Неотредактированные данные WHOIS ранее указывали на векторы атак, с которыми сообщество ICANN имеет дело уже более десяти лет. Взлом домена, спам, фишинг, телефонное мошенничество, поддельные уведомления о продлении. Все,

о чем мы говорим на протяжении десятилетия с лишним, можно решить, защитив регистрационные данные от полного доступа для всех.

Кроме того, как мы снова и снова слышим, общий объем злоупотреблений доменными именами не увеличивается. Он снижается. И во время пандемии COVID-19 общего роста не было.

Дальше, пожалуйста.

Я просто привожу это здесь в качестве общей информации. Для тех, кто заинтересован в подаче запросов на данные, это своего рода минимум и лучшая информация, которую кто-то может предоставить регистратору или регистратуре при подаче запроса на раскрытие данных. Он основан на заключительном отчете по фазе 2 EPDP, а также на передовых методах, наработанных регистраторами и регистратурами. И есть ссылка, прямая ссылка на это на сайте группы заинтересованных сторон-регистраторов, которую я поместил туда. Но это просто дает некоторую базовую минимальную информацию, которую сторона, связанная договорными обязательствами, должна будет просмотреть, чтобы провести балансирующий тест на необходимость раскрытия информации. А без этой информации процесс замедлится.

И, да, регистраторы и регистратуры получают жалобы без указания доменного имени или без указания законного права, на основании которого подается запрос, или без каких-либо элементов данных. И это задерживает процесс. Таким образом, вам просто нужна полная информация, чтобы регистратор или регистратура могли оказать помощь и быстрее принять решение о раскрытии.

Следующий слайд, пожалуйста.

Итак, теперь я собираюсь просто сделать обзор некоторой информации, которая была собрана для нашей презентации, данные были добровольно предоставлены некоторыми регистраторами и регистратурами. Здесь представлены малые, средние и крупные регистраторы и регистратуры, а также несколько географических регионов мира. У нас был широкий диапазон данных, поэтому некоторые регистраторы сообщили всего лишь о 30, а другие – о 3400 запросах. У регистратур показатели были ниже, а первоначальные цифры после GDPR были выше, но с тех пор они как бы выровнялись.

Таким образом, некоторые ключевые выводы заключаются в том, что менее 1% от общего числа управляемых доменов подвергались запросам, и они варьировались в зависимости от типа редактирования, поскольку различные стороны, связанные договорными обязательствами, реализовали и адаптировали временную спецификацию и другие вещи.

Я также хотел бы подчеркнуть, что в рамках SSAD будет гораздо больше показателей, требуемых ICANN, о которых также будет сообщаться ICANN, а затем сообществу. Таким образом, после создания SSAD мы сможем лучше понять, какие типы запросов на раскрытие поступают, кто это делает, каковы результаты и так далее.

Следующий слайд, пожалуйста.

Итак, вот некоторые из результатов, которые мы увидели. Таким образом, вы можете видеть, что регистратуры примерно в половине случаев отклоняли или перенаправляли запросы, а регистраторы примерно две трети запросов отклоняли или перенаправляли.

Перенаправление означает, что регистратура предлагает обратиться к регистратору, или что отказано по причине незаконности. Здесь тест на балансировку.

Некоторые из других причин, по которым информация не обязательно раскрывается – это защита домена услугой сохранения конфиденциальности, или домен не зарегистрирован у этого регистратора или регистратуры.

Следующий слайд, пожалуйста.

Какие данные были предоставлены? В одной трети случаев это были данные о владельце домена, а в двух третях – данные

администратора и технические данные владельца домена. И вообще, когда данные не разглашались, стандартной практикой было дать какое-то обоснование и объяснение. Знаете, часто, когда сервис сохранения конфиденциальности / регистрации через доверенных лиц делает запрос на раскрытие данных, это не лучший способ сделать это. У служб сохранения конфиденциальности / регистрации через доверенных лиц есть свои собственные процессы и процедуры для этого.

Следующий слайд, пожалуйста.

Таким образом, некоторые регистраторы действительно получали апелляции на отклонение запросов на раскрытие информации. У регистратур их не было. Вы видите, что количество регистраторов очень мало. Часто запросы, поступающие через апелляцию, поступают по неправильному механизму и обычно приводят к просветительской работе или объяснению того, почему в этом конкретном случае было отказано. И примечательно, что ни одна из апелляций не отменила решение о раскрытии информации или его отсутствие.

Следующий слайд, пожалуйста.

Итак, вот некоторая информация о типах предоставленных запросов. Вы видите, что около трех четвертей из них были от правоохранительных органов – извините, это были IP-запросы, около 15% – от правоохранительных органов, а остальные

были другими, включая исследователей в сфере безопасности, запрос без домена (неразборчиво) или, опять же, домены которые не были у регистратора или регистратуры.

Следующий слайд, пожалуйста.

Итак, из всех запрашивающих, которые у нас есть, я вижу, что один... один податель запроса приходился на каждые четыре запроса. То есть много повторных запросов. Фактически, один конкретный податель запроса был источником 45% запросов, что составляет значительную часть всего общего объема запросов.

Так что я думаю, что это... еще один слайд, пожалуйста.

Это был типичное время ответа. В целом это длилось менее трех дней. Регистратуры работали немного быстрее, чем регистраторы, потому что часто именно регистратура перенаправляла запрашивающего к регистратору, находится в лучшем положении, владея данными, либо принимая решение о раскрытии.

На этом я подошел к концу. Надеюсь, я рассказывал не слишком быстро. Я просто хотел, чтобы у нас было достаточно времени для дальнейшего обсуждения.

Спасибо.

ДЖОНАТАН ЗУК: Спасибо, Оуэн. Я знаю, что тебе пришлось многое пережить за короткое время. Так что я ценю, что ты быстро с этим справился. Это очень полезные данные.

ОУЭН СМИГЕЛЬСКИ: И, пожалуйста, взгляните на тот сентябрьский вебинар. Это был полуторачасовой вебинар, поэтому мне пришлось немного ужать материал. Там была хорошая дискуссия и много информации. Спасибо.

ДЖОНАТАН ЗУК: Определенно было. Возможно, персонал, если бы вы могли найти для этого ссылку на запись Zoom и опубликовать ее в чате, это было бы хорошо. Думаю, это очень хороший фон для этих разговоров. И я ценю, что стороны, связанные договорными обязательствами, собрали эти данные.

Мы собираемся сделать резервную копию слайдов, я думаю, немного, персонал, потому что Марк Сванкарек присоединился к телеконференции, и мы хотим дать ему возможность коротко выступить.

Итак, Марк, без лишних слов, приступайте.

МАРК СВАНКАРЕК: Спасибо всем. Вы меня слышите?

ДЖОНАТАН ЗУК: Слышим.

МАРК СВАНКАРЕК: Извините. У меня сломался будильник. Что за выступление любителей, а?

Привет, я Марк Сванкарек из Microsoft, и я здесь, чтобы дать общее представление о том, как мы в Microsoft видим киберпреступность и что происходит с WHOIS и GDPR.

Так что я постараюсь действовать быстро, чтобы мы могли перейти к... (смех)... разговору.

Я кое что выкладываю в чат. Это новый отчет Microsoft по цифровой защите. Мы это делаем впервые. Он довольно подробный и рассказывает, как мы видим текущее состояние киберпреступности.

Сейчас много говорят о том, выросла или уменьшилась киберпреступность в последнее время. Я не уверен, почему это дебатируется. Она растет. Растут все виды киберпреступности. И поэтому защита от нее остается высоким приоритетом, и для этого требуется много усилий.

Набор данных WHOIS – это один из методов, который мы используем для борьбы со всеми видами преступлений, корпоративного мошенничества, обмана потребителей, для

борьбы с пиратством, оценки угроз для государственных органов и многого другого.

Прошу прощения.

Да, я не предоставил слайды. Прошу прощения. Когда я предварительно просматривал слайды, мне показалось, что их представил только Милтон. Поэтому я подумал, что это будет просто разговор.

Так что... Извините.

В любом случае, проблема, с которой мы сталкиваемся в отношении WHOIS в соответствии с GDPR прямо сейчас, заключается в том, что мы на самом деле не разработали систему, которая позволяет нам получать доступ к данным в полном объеме, который будет разрешен в соответствии с правилами. И я думаю, что было бы интересно продолжить обсуждение этого вопроса в группе, но на самом деле все сводится к тому, что мы получили определенный объем юридической информации. И внутри группы не было единого мнения о том, что на самом деле означает эта юридическая обратная связь. И это в отношении точности, необходимости и тому подобного.

И поэтому я думаю, что если вы посмотрите сентябрьский вебинар, уделите примерно 34 минуты фактическому процессу, который предлагается для тестов балансировки, я

думаю, вы увидите, что он сильно отличается от отзывов, которые мы получили от Bird & Bird о том, что значит «необходимо». Итак, у меня есть часть этой информации, если вы посмотрите... где же это? Прошу прощения. У меня нет готовых ссылок. Я думал, приготовил их. В общем, я приношу извинения. Мне действительно очень жаль, ребята.

Я выложу это все в чат через минуту. Но в основном это сводится к необходимости... я действительно собираюсь вставить здесь свою цитату.

Можно двигаться дальше.

О боже. О боже. О боже. Пока я ищу ссылку, дело в том, что мы слышали такие вещи, как существование разрешения споров, таких как UDRP, и это означает, что раскрытие данных, например, в WHOIS, никогда не было бы законным. Это не так.

ДЖОНАТАН ЗУК: Эй, Марк. Это Джонатан.

МАРК СВАНКАРЕК: Знаешь, я вернусь через минуту.

ДЖОНАТАН ЗУК: Нет необходимости делать ссылки активными. Если есть какие-то важные моменты, которые вы хотели бы высказать, я думаю, можете это сделать тут. Но мы также можем, в противном случае, просто продолжить обсуждение.

МАРК СВАНКАРЕК: Давайте продолжим обсуждение. И я очень скоро найду эти ссылки.

Но дело в том, что было много утверждений о том, что SSAD можно разработать только одним способом из-за полученных нами юридических отзывов. А это не так. На самом деле у нас были дополнительные возможности, и мы решили не использовать их.

И путь...

ДЖОНАТАН ЗУК: Благодарю вас, Марк. Я думаю, что в этом решении мы действительно хотим сосредоточиться не на повторном подтверждении этого, а на том, чтобы посмотреть, какими были эти запросы, сроки и т. д. Вот почему данные Оуэна были так полезны.

Я знаю, что Дэвид Тейлор собрал некоторые данные о запрашивающей стороне.

Учитывая тот факт, что GDPR – это реальность, учитывая тот факт, что вы знаете, что его соблюдение – это реальность, реализация рекомендаций EPDP – это реальность, каналы, есть ли каналы связи между подателями запросов и держателями данных, если нет лучшего термина?

Я думаю, что это именно тот разговор, который мы хотим провести, каким был этот обмен, забегая вперел. Вот почему данные Оуэна были очень полезны.

Потому что, например, одна из вещей, которая возникла в начале презентации, была идея, которую, я думаю, упомянул Габриэль, а именно, что к тому времени, когда что-то замечается – фишинговое мошенничество замечается, оно уже закончилось, то есть можно предположить, что у сторон, связанных договорными обязательствами, недостаточно времени, чтобы ответить вам, например, после жалобы.

И поэтому я думаю, что мы хотим начать настоящий разговор о том, что реально с точки зрения того, как может выглядеть этот обмен данными.

Итак, давайте посмотрим. Да, поэтому один из разговоров, который возникал довольно часто, заключается в том, что данные DAAR, похоже, предполагают, что неправильное использование DNS в целом уменьшилось. Тем не менее,

похоже, есть и другие данные о том, что оно увеличилось или выросло по разным направлениям, и так далее.

Есть ли кто-нибудь, кто хочет прокомментировать эту идею? Это от Люка Сейфера, который задал вопрос в блоке вопросов. Почему существует дихотомия между этими двумя разными наборами данных? Почему у нас нет окончательного ответа о том, в каком направлении идет неправильное использование DNS?

ГРЕГ ААРОН (GREG AARON): Привет, Джонатан. Это Грег. Я могу говорить об этом, потому что я разработал и построил систему DAAR.

DAAR рассматривает данные из нескольких разных списков блокировки, содержащих доменные имена. И она смотрит на списки блокировки, которые охватывают определенные категории явлений, таких как фишинг и вредоносное ПО.

Обычно мы ожидаем, что со временем будут возникать подъемы и спады. Если на какое-то время уровень снизится, он может снова увеличиться. Это своего рода стандарт.

Так что она измеряет очень конкретные вещи из очень конкретных источников. Однако мы видим, что новые методы уклонения могут уменьшить количество видимых вами доменов. Мы не знаем, к чему приводит меньшее количество доступной информации WHOIS, как это повлияло на

эффективность блокирования. Хотя некоторые источники измерили это, и есть некоторые публикации, которые показывают, что, если будет труднее найти плохих парней, вы получите меньше доменов в списке заблокированных. Это один из возможных эффектов.

Так что это не означает, что количество киберпреступлений снизилось. Это просто означает, что вы нашли меньше доменов и меньше в просматриваемых списках.

Когда Оуэн говорит, что общее злоупотребление доменными именами сокращается, это может быть по одному из критериев в зависимости от определенных обстоятельств и определенных источников.

Тем не менее, как ни измерять, все равно это много. Еще одна вещь, о которой следует помнить – это то, что количество доменных имен в данном списке не является мерой нанесенного ущерба или связанного с этим риска. Например, из-за компрометации корпоративной электронной почты сумма денег, теряемых в результате каждого из этих видов мошенничества, в среднем растет. Так что, если у вас такое же количество доменных имен, ущерб для жертв будет больше.

Так что я думаю, это действительно зависит от того, что вы измеряете и как. Другие индикаторы говорят, что уровень

растет. Итак, DAAR делает что-то определенным образом. И я не думаю, что это, показательно для всей экосистемы. Спасибо.

ДЖОНАТАН ЗУК: Спасибо, Грег. Тео Гертс спросил: Каково качество данных, раскрываемых регистратором? Можно ли их использовать для расследований?

Мы слышали от ряда людей, что дела уже ухудшились из-за недостаточной точности, конфиденциальности, услуг сохранения конфиденциальности и регистрации через доверенных лиц и так далее. Можете ли вы... я думаю, как спросил Милтон: Можете ли вы действительно объяснить трудности, с которыми вы сталкиваетесь, изменениями, которые произошли в результате соблюдения GDPR? Я думаю, этот вопрос предназначен как для специалистов, занимающихся исследованиями в области кибербезопасности, так и для правоохранительных органов.

ГАБРИЭЛЬ ЭНДРЮС: Здравствуйте. Это Габриэль. Если я могу вставить слово, просто дам на это небольшой ответ.

ДЖОНАТАН ЗУК: Пожалуйста.

ГАБРИЭЛЬ ЭНДРЮС: Я думаю, что качество ответа, очевидно, будет разным, но его всегда стоит получать. И действительно, единственный раз, когда ответ ничего не стоит – это если он просто возвращается к службе сохранения конфиденциальности / регистрации через доверенных лиц, которая ничего вам не скажет. Но мы обнаруживаем, что даже если преступники лгут о своих регистрационных данных или использовали скомпрометированные платежные данные и т. д., это все элементы данных. И вы никогда не знаете, какой элемент данных на самом деле будет ключевым для запуска расследований. Поэтому я бы предпочел получить даже мошеннические данные о владельце домена, чем не иметь доступа к ним. Хотя, очевидно, чем больше эти данные проверяются при регистрации, тем лучше для нас и хуже для преступников.

Спасибо, Габриэль.

Стефани Перрен задала вопрос: Есть ли у нас статистика по частоте кражи достоверных данных и их подмены данными преступников? Исторические данные уже наскребли. Многое еще актуально.

ГРЕГ ААРОН (GREG AARON): Это Грег. Я могу ответь на это. Здравствуйте, Стефани.

ДЖОНАТАН ЗУК: Великолепно, спасибо.

ГРЕГ ААРОН (GREG AARON): Я имею в виду, что я просмотрел контактные данные буквально миллионов доменных имен, неправильно использовавшихся на протяжении многих лет. Я вижу, что преступники не склонны извлекать данные других людей и использовать их. Они склонны просто выдумывать данные. И некоторые справляются с этим лучше, чем другие. Из моего личного опыта – относительно редко можно увидеть просто незаконно присвоенные данные.

ДЖОНАТАН ЗУК: Ладно. Спасибо.

Не можете ли вы включать камеру, когда говорите? Мы пытаемся показывать больше лиц на таких онлайн-заседаниях. Так что, когда вы отвечаете на вопрос, было бы здорово, если бы вы могли включить камеру. Я знаю, что это потребует много щелчков взад и вперед, но в идеале люди могут их видеть.

Фолькер упомянул: Грег, кажется, говорит, что нет никакой пользы от блокировки доменных имен после получения сообщения, поскольку ущерб уже нанесен. Это кажется нелогичным.

ГРЕГ ААРОН (GREG AARON): Нет. Я думаю, что Фолькер неправильно это понимает. Одна из вещей, которые вы увидели в той диаграмме, которую я показал, это то, что да, если вы действительно заблокируете домен, вы получите дополнительную выгоду. Кроме того, фишинг – это один из самых кратковременных видов киберпреступлений. Таким образом, вы получаете гораздо больше преимуществ, когда приостанавливаете доменное имя, зарегистрированное преступником, поэтому это очень полезно.

Однако вопрос, безусловно, в том, что есть разница между смягчением последствий и предотвращением. Одна из вещей, которые мы увидели из данных, это наличие определенных мест, куда преступники заходят и регистрируют доменные имена. Их домены приостанавливаются, а затем они просто регистрируют новые. У нас действительно есть проблема с повторными действиями. И было бы здорово, если бы можно было выявлять и предотвращать больше повторных действий на раннем этапе.

Так что предположить, что приостановка доменных имен ничего не стоит, нет, это точно того стоит.

Опять же, цель игры здесь – защитить людей, которые становятся жертвами.

МИЛТОН МЮЛЛЕР: Могу я подключиться, Джон?

ДЖОНАТАН ЗУК: Конечно, Милтон. Вам слово.

МИЛТОН МЮЛЛЕР: Опять же, я думаю, что нам действительно нужно сосредоточиться на скрытии данных до и после WHOIS. Вот в чем проблема. Я не думаю, что есть смысл говорить, что фишинг – это проблема. Все мы знаем это.

Вопрос в следующем: Насколько борьба с фишингом или другими формами киберпреступности действительно полагается на открытый доступ к данным WHOIS?

И я думаю, что злоумышленники придумали довольно надежные методы предотвращения обнаружения, и большинство реальных тормозов, которые накладываются на фишинговые домены, исходят от приостановки и от алгоритмов, обнаруживающих шаблоны и быстро блокирующих их. И мне неясно, связано ли с этим наличие или отсутствие данных WHOIS. И снова, глядя на данные, мы не видим статистической корреляции между проблемами до и после WHOIS. Так что давайте сосредоточимся на этом.

Я не думаю, что можно просто сказать, что нам нравилось, когда у нас был такой доступ. Но когда у вас был такой доступ к данным, неизбирательный, открытый, фишинг все еще был проблемой. Это была очень быстрорастущая проблема, и она росла быстрее, чем сейчас.

Так что давайте снова сосредоточимся на причине и следствии, если сможем.

ДЖОНАТАН ЗУК: Отличный вопрос, Милтон. Кто-нибудь хочет ответить на это со стороны правоохранительных органов или со стороны кибербезопасности?

ГАБРИЭЛЬ ЭНДРЮС: Что ж, я могу добавить комментарий, что отсутствие этих данных отрицательно сказывается на расследованиях. Есть много причин, почему это происходит, но, возможно, это более обширный разговор.

Я хотел бы упомянуть эту группу и свои предыдущие комментарии о том, что наши обязанности включают не только сторону атрибуции, но также иногда включают быстрое уведомление потенциальных жертв. И это реальный пример, когда мы абсолютно уязвимы и что мы используем не только идентификаторы субъектов в системе DNS, но и идентификаторы, связанные с жертвами, на которые активно нацелены атаки. И это предположительно достоверные данные. Но если они недоступны в кратчайшие сроки, то важные разговоры, которые могут происходить по телефону с кем-то, чьи учетные записи электронной почты потенциально скомпрометированы и становятся целью прямо тогда, в тот же

день или на следующий день, они позволяют нам вести эти разговоры. А если не сможем, то не сможем и в ущерб гражданам во всем мире.

ДЖОНАТАН ЗУК: Габриэль, вы предполагаете, что тогда использование данных более ценно для установления связи с невиновными, чем для отслеживания преступников?

ГАБРИЭЛЬ ЭНДРЮС: Я не думаю, что могу делать оценку. Я могу просто сказать, что знаю, что они используются для обоих, если это честно. Я не... мне трудно делать широкие, общие заявления о том, что происходит, просто потому, что я пытался собрать данные и видел, как трудно заставить следователей отвлечься от своих дел, чтобы сделать отчет. Например, я 82 раза пытался получить информацию о владельце домена, и у меня получилось в 42 случаях. Верно? Они не отслеживают неудачи. Поэтому очень сложно вернуться и предоставить факты, которые, как я знаю, были бы здесь чрезвычайно полезны.

Но я могу сказать, что, когда я собирал эти данные, меня больше всего поразило разочарование, которое испытывали некоторые следователи, которые пытались поступить правильно, уведомить людей, которым будет причинен вред, и они обнаруживали, что оказались в тупике. И это не значит,

что они не могли каким-то образом исследовать другие возможности.

Это просто говорит о том, что это самый быстрый метод, который раньше работал у них, но теперь это не так. И это то, на что я хотел обратить внимание.

И теперь можно двигаться дальше.

ДЖОНАТАН ЗУК: Спасибо. Габриэль.

Оуэн, я знаю, что в той части презентации, которая была недавно проведена сторонами, связанными договорными обязательствами, о доступе к данным, были заложены некоторые основы для улучшения форматирования запросов с целью их ускорения и т. д. Есть ли какие-либо примеры или какие-либо данные, связанные с тем, что податели запросов делают это таким образом?

И есть ли тогда корреляция с большей вероятностью того, что данные будут предоставлены более оперативно?

ОУЭН СМИГЕЛЬСКИ: Спасибо, Джонатан. Для протокола – это Оуэн Смигельски. Я не могу сделать из этого никаких выводов. Конечно, это был конечный и необязательно исчерпывающий набор данных, но

опыт сторон, связанных договорными обязательствами, показал, что когда у них действительно были запросы с дополнительной информацией, они могли обрабатывать их быстрее. Они смогли быстрее провести надлежащие тесты балансировки. Но то, что вы предоставляете всю информацию, не означает, что запрос пройдет этот тест на балансировку. Существуют ли менее интрузивные способы решения проблемы, чем просто получение данных? Здесь есть ряд вопросов и факторов, которые могут быть применимы.

Это, безусловно, ускоряет процесс. Это может привести вас к выводам. Большая часть данных показывает, что большинство запросов касается нарушения прав на товарные знаки. Так что, как правило, это не обязательно один из тех срочных случаев, когда необходимо удалить ботнет. Есть и другие пути, такие как UDRP или URS, или аналогичные вещи, для которых вам не нужны данные. Таким образом, это менее интрузивный способ, который, таким образом, прошел бы... он не прошел бы этот тест на балансировку, потому что есть менее интрузивные средства для этого.

ДЖОНАТАН ЗУК: Оуэн, как вы думаете, будет ли тест балансировки по-прежнему полностью индивидуальным, или будет какой-то способ, например, чтобы люди, которые подписались на структуру защиты от неправильного использования DNS,

собрались вместе и создали какое-то дерево решений, которое делает его немного менее черным ящиком для людей, которые пытаются получить данные от сторон, связанных договорными обязательствами?

ОУЭН СМИГЕЛЬСКИ: Спасибо, Джонатан. Это снова Оуэн, для стенограммы.

Я не могу точно сказать, что произойдет в будущем. По-прежнему существует неоднозначность и неуверенность в том, что нельзя разрешать. Некоторые из уже существующих рекомендаций заключаются в том, что некоторые вещи нельзя автоматизировать. А с запросами на раскрытие данных так много неизвестного.

Я видел какой-то чат, в котором говорилось, что Конгресс США собирается принять некое решение, чтобы сделать WHOIS общедоступной. Но для крупного регистратора, такого как Namecheap, где у нас миллионы клиентов по всему миру, не всегда возможно со 100-процентной уверенностью сказать, что это человек, который находится за пределами юрисдикции, это не связано с проблемой конфиденциальности данных, и разглашение этих данных может повлечь за собой гражданскую и уголовную ответственность. Так что это не формочка для печенья, которую можно легко сделать универсальной для всех случаев. Некоторые регистраторы

могут быть меньше по размерам, ориентироваться только на определенный регион или использовать другую бизнес-модель.

Поэтому я думаю, что по мере того, как это развивается с течением времени, и это, безусловно, встроено в SSAC для ее развития и изменения в процессе разработки политики, я думаю, что это, безусловно, будет развиваться, но еще слишком рано предсказывать, как это пойдет.

Спасибо.

ДЖОНАТАН ЗУК: Спасибо, Оуэн. Думаю, по тому же вопросу: Лори Шульман спросила, готовы ли вы обсудить конкретный опыт Namecheap с точки зрения количества полученных запросов и того, сколько из них привело к раскрытию данных.

ОУЭН СМИГЕЛЬСКИ: Привет, Джонатан. Это снова Оуэн. Я не могу обсуждать это прямо здесь. У меня сейчас нет доступа к этим данным.

ДЖОНАТАН ЗУК: Отлично. Спасибо.

Итак, я знаю, что был разговор, я пытался просмотреть все блоки вопросов и чат, чтобы попытаться понять, о чем говорит сообщество в целом. Я знаю, что Майк Грэм, если вы подключены, вы задали конкретный вопрос о конкретном изменении, которое произошло с редактированием. Вы хотите включить микрофон и поделиться с нами этим? Потому что это просто проскочило в чате.

Не хочу поставить вас в неловкое положение.

Да, можете ли вы включить свой микрофон, или могут сотрудники разрешить Майку включить его микрофон?

МАЙКЛ ГРЭМ (MICHAEL GRAHAM): Теперь работает?

ДЖОНАТАН ЗУК: Да. Спасибо.

МАЙКЛ ГРЭМ (MICHAEL GRAHAM): Извините. Действительно быстро, я могу поделиться только небольшой информацией в плане усилий и затрат. И есть два разных способа, которые сработали. Один из них заключается в простом обнаружении информации, чтобы мы могли определить, было ли конкретное доменное имя зарегистрировано и используется обманным путем, или,

возможно, оно может быть зарегистрировано кем-то, кто связан с нашей компанией, и это просто означает, что они непреднамеренно допустили тайпсквоттинг.

И, конечно же, в последнем случае мы понимаем, что есть много людей, которые выходят в Интернет, они не искушены и могут делать что-то, что, как вы знаете, может повредить не только нашей способности связываться с потребителями и тому подобное, но (неразличимо) их способности делать это и быть добропорядочным интернет-гражданином, но с точки зрения просто исследований и затрат для компаний, получение этой информации – это огромные затраты, дополнительные расходы. А с точки зрения реального злоупотребления – и это злоупотребление не обязательно фишинг, но в некоторых случаях это фишинг для нас, а в других случаях просто откровенная подделка, которая распространяется в Интернете. Стоимость расследований сильно возросла. И в какой-то момент это цена, которую платим не только мы, но и потребители, как с финансовой точки зрения, так и с точки зрения их способности доверять тому, что они находят в Интернете. И это то, что нас действительно беспокоит, то, что они могут найти то, что ищут, и не быть обманутыми в одной из этих схем, которая, кажется, продолжается изо дня в день.

ДЖОНАТАН ЗУК: Спасибо, Майкл.

Вопрос стоимости – сложный, потому что очевидно, что податели запросов не всегда чувствительны к затратам, возлагаемым на стороны, связанные договорными обязательствами. Чтобы реализовать некоторые из вещей, которые от них просят.

Так что если соблюдение закона – это просто затраты на ведение бизнеса, то я думаю, что это... это тоже будет сложным вопросом баланса.

Элизабет...

МИЛТОН МЮЛЛЕР: Могу я подключиться?

ДЖОНАТАН ЗУК: Да, Милтон. Вам слово.

МИЛТОН МЮЛЛЕР: В некотором смысле речь идет о затратах, потому что на протяжении 20 лет податели запросов не только получали бесплатный обед, но и субсидировались режимом ICANN. Мы в основном предоставляем владельцам доменных имен договор присоединения, в котором говорится, что вы хотите доменное имя, и от вас требуется, без вашего согласия, без какого-либо участия в этом вопросе, сделать вашу личную

информацию глобально доступной для всех, кто этого захочет. И это требовало затрат со стороны владельцев доменов, и это субсидировало доступ людей, некоторые из которых собирали эту информацию, продавали ее и зарабатывали на этом деньги.

И я думаю, что... с помощью SSAD мы сказали – хорошо, затраты будут сбалансированы более справедливым и более эффективным способом. Если вы большой заказчик, и мы все можем вспомнить пару компаний, которые генерируют большую часть запросов, я думаю, что данные Оуэна действительно очень помогли в этом, вы тот, кто генерирует затраты на систему. Вы, так сказать, виновник затрат и должны платить больше. Вы должны поддерживать систему либо за счет платы, создаваемой пользователем, либо за счет какой-либо многоуровневой платы за аккредитацию, которая покроет стоимость предоставления этих данных.

И если эти данные будут доступны так быстро, как хотелось бы некоторым людям, очевидно, что вы возлагаете огромные расходы на сторону, связанную договорными обязательствами, которой нужно, чтобы кто-то сидел и оценивал эти запросы. И опять же, вы можете избежать некоторых из этих затрат за счет автоматизации, но автоматизация также может быть незаконной, если вы на самом деле не выполняете надлежащую проверку характера запроса.

Так что, как вы говорите, это действительно сложная задача, Джонатан, и я думаю, что... с точки зрения целей этой группы, я думаю, было бы хорошо иметь больше информации о том, как сбалансированно затраты распределяются среди различных групп заинтересованных сторон.

ДЖОНАТАН ЗУК: Спасибо, Милтон.

Натали Леруа спрашивает: Большинство европейских регистратур предлагают услугу публикации данных в соответствии с GDPR, если податель запроса может предоставить доказательства регистрации товарного знака. Думают ли gTLD или другие ccTLD о принятии аналогичной модели? Это очень помогает усилиям по обеспечению соблюдения требований.

Оуэн, возможно, вы единственный, кто сможет ответить на этот вопрос, даже если не знаете ответа.

ОУЭН СМИГЕЛЬСКИ: Прошу прощения. Я пытался следить за чатом. Какой был вопрос?

ДЖОНАТАН ЗУК: Извините, Натали Леруа. Это в самом низу блока вопросов.

ОУЭН СМИГЕЛЬСКИ: Я не знаю, спасибо. Это Оуэн — для стенограммы.

Я не уверен, есть ли другие gTLD или ccTLD, которые применяют аналогичные модели, но по мере того, как все это развивается и мы входим в эту SSAD, может быть появиться способ проверки пользователей для конкретного gTLD, либо что-то в этом роде.

Опять же, отправной точкой стал отчет о фазе 2 EPDP. Некоторое время мы испытывали давление, чтобы все было сделано, все предусмотрено. Было много участников внутри и снаружи, которые хотели, чтобы что-то было сделано быстрее, чем то, что мы делаем, и поэтому мы сделали все, что могли, в то время, которое у нас было.

Так что я думаю, что это, безусловно, могло бы быть предложением, продвигающим дело вперед, поскольку модель SSAD действительно развивается, чтобы что-то там добавить. Я думаю, что если это согласовано и соответствует законам, то это, безусловно, может облегчить (неразборчиво).

Спасибо.

ДЖОНАТАН ЗУК: Спасибо, Оуэн.

Надеюсь, это поможет, Натали. Я думаю, что это гораздо более серьезный вопрос, чем мы можем решить сегодня.

Лорин попросила разрешение ответить Милтону. Лорин, вам слово. Или, персонал, вы можете включить микрофон Лорин.

ЛОРИН КАПИН: Я думаю, что звук уже включен.

ДЖОНАТАН ЗУК: Что ж, превосходно.

ЛОРИН КАПИН: Спасибо. И я хотела согласиться с некоторыми замечаниями Милтона о том, что эта информация является палкой о двух концах. И, конечно, его можно использовать в плохих целях. И действительно, Милтон, мы видим это и в данных о жалобах.

Но с другой стороны, DNS – это общедоступный ресурс. И Милтон привел пример того, как вещи собираются и используются в злонамеренных целях, что противоречит закону, с чем нет разногласий.

Но GDPR не защищает данные юридических лиц. И я с нетерпением жду продолжения усилий по разработке политики в этом отношении, потому что общественность имеет

право знать информацию юридических лиц. И это изменение, позволяющее пользователям узнавать, кто стоит за доменами, которые не являются индивидуальными организациями, будет иметь большое значение для помощи общественности и правоохранительным органам в их расследованиях и усилиях по комплексной проверке.

И точно так же, как мы требуем предоставления определенной информации для использования общедоступных ресурсов, будь то водительские права или бизнес-лицензия, и некоторая часть этой информации становится общедоступной, это следует делать для юридической информации, связанной с юридическими лицами.

ДЖОНАТАН ЗУК: Спасибо, Лорин.

Есть еще вопросы, персонал будет их собирать, и мы постараемся найти способ записать ответы. К сожалению, у нас закончилось время. Это был хороший разговор. Всегда сложно сохранять сосредоточенность. И... но, отвечая на вопрос Джеффа о цели пленарного заседания, я не уверен. Но в идеале, чем лучше мы понимаем фактическую ситуацию до и после изменения в политике ICANN, тем лучше мы будем информированы о том, какие шаги необходимо предпринять дальше. И я думаю, что целью данного обсуждения было,

насколько это возможно, понять, к чему привело это изменение статус-кво с точки зрения потока данных и доступности информации, необходимой для защиты потребителей в исследованиях кибербезопасности.

Надеюсь, это была миссия по установлению фактов. Очевидно, что предстоит еще многое узнать. В модуле осталось много вопросов. Мы посмотрим, что мы можем сделать для их рассмотрения, но сегодня у нас время закончилось. Для меня сейчас 3 часа ночи, так что у меня, вероятно, закончились остроумные высказывания, поэтому я просто скажу спасибо всем докладчикам и всем людям, которые присоединились к нам, чтобы обсудить это. Мы просмотрим чат и т. д. и будем использовать это как топливо для дальнейших разговоров.

Еще раз большое спасибо всем. Объявляю заседание закрытым.

[КОНЕЦ СТЕНОГРАММЫ]