



25 февраля 2009 г.

SAC 038: Канал связи регистратора для борьбы с нарушениями

Введение и историческая справка

Действующие соглашения ICANN по рДВУ требуют от реестров и регистраторов обязательного использования данных службы "Кто есть кто" (Whois). Статья 3.3.1¹ Договора об аккредитации регистратора определяет, какие контактные сведения регистраторы и их агенты (реселлеры) должны получать от заявителей при регистрации доменного имени. Регистрационные контактные сведения служат основным средством связи с заявителем на доменное имя или оператором (администратором) Интернет-хоста (сервера), которому присвоено имя в данном домене. Возможные причины, по которым может потребоваться связь со сторонами, обозначенными в качестве контактных лиц для доменного имени: общие запросы (напр., в отношении бизнеса), попытки уведомить заявителя об ошибках в конфигурации DNS и запросы по поводу возможного отношения доменного имени к злоумышленной, противозаконной и преступной деятельности.

Правоохранительные органы, группы быстрого реагирования на нарушения компьютерной безопасности (CERT), сообщества по борьбе с фишинг-мошенничеством и преступной деятельностью (третьи лица), компании, предлагающие услуги защиты репутации в Интернете, сетевые операторы и пользователи Интернета могут попытаться связаться с аккредитованными регистраторами ICANN при невозможности выйти на связь с хозяином домена с помощью контактной информации, полученной в базе данных службы "Кто есть кто" (Whois). В случае родовых ДВУ в записях службы "Кто есть кто" (Whois) обязательно должно быть указано имя аккредитованного регистратора ICANN (спонсирующий регистратор). Следовательно, у пользователей всегда должна быть возможность получить имя регистратора, спонсирующего доменное имя, путем запроса информации о регистрации доменного имени через службу "Кто есть кто". Затем пользователь должен иметь возможность найти контактную информацию службы по борьбе с нарушениями этого регистратора из нескольких источников.

Сводные списки с контактной информацией регистраторов существуют, однако не все лица, указанные в этих списках, могут рассматривать жалобы на нарушения и разбирать обвинения в преступной деятельности. В случаях, когда на веб-сайте регистратора явным образом обозначена контактная информация отдела,

¹ См. ссылку <http://www.icann.org/en/registrars/ra-agreement-17may01.htm#3.3.1>.

Канал связи регистратора для борьбы с нарушениями

отвечающего за борьбу с нарушениями, третьи лица зачастую обращаются к соответствующему представителю регистратора. Если же контактную информацию отдела по борьбе с нарушениями трудно найти на веб-сайте регистратора, поиск нужной информации пользователем приводит к задержкам в разрешении споров и рассмотрении жалоб о нарушениях.

Кроме того, контактные сведения регистраторов можно найти в открытом списке ICANN. Регистраторы предоставляют корпорации ICANN основную контактную информацию в целях получения уведомлений в соответствии с контрактами. По контракту регистраторы не обязаны предоставлять контактную информацию в открытый доступ и выделять отдельного сотрудника для рассмотрения нарушений. В настоящий момент корпорация ICANN позволяет регистраторам предоставлять вместо основной (контрактной) альтернативную контактную информацию для открытого доступа и публикует эту альтернативную информацию². Если регистраторы не предоставляют корпорации ICANN специальную информацию для открытого доступа, на веб-сайте ICANN публикуется основная контактная информация. Еще раз уточняем, что канал связи, представленный в списке ICANN, может не быть лицом, уполномоченным для рассмотрения жалоб о нарушениях и обвинений в преступной деятельности.

Проблемы

Принятые в настоящий момент требования к публикации контактной информации в открытом доступе могут не соответствовать потребностям сообщества по следующим причинам:

- Для регистраторов публикуется информация о каналах связи разного рода. Не все эти каналы связи предназначены для рассмотрения жалоб о нарушениях и обвинений в преступной деятельности. Поиск нужного контакта может привести к задержкам в рассмотрении вопроса.
- Пользователям, делающим запросы или рассматривающим потенциальное участие доменного имени в нарушениях и преступной деятельности, приходится полагаться на добровольно публикуемые регистраторами каналы связи, которые должны постоянно обслуживаться. В ККБС поступает анекдотичная информация:
 - a) Не все регистраторы добровольно публикуют на своих веб-сайтах открытую контактную информацию;
 - b) Не вся опубликованная контактная информация является точной и полной;
 - c) Персонал, чья контактная информация опубликована, может не иметь полномочий для рассмотрения запросов о нарушениях или не иметь представления о том, к какому лицу (напр., техническому специалисту) следует направить запрашивающего;

²

См. ссылку <http://www.internic.net/regist.html>.

Канал связи регистратора для борьбы с нарушениями

- d) И не все регистраторы публикуют информацию об особом контактном лице, которое занимается вопросами нарушений.
- В некоторых случаях открытый канал связи работает только в определенные рабочие часы, в то время как персонал по борьбе с нарушениями должен быть доступен 24 часа 7 дней в неделю. Обычно заявления о предполагаемых нарушениях или преступной деятельности требуют своевременного, а то и незамедлительного ответа. Например, случаи, когда необходима приостановка работы доменного имени, используемого для фишинг-мошенничества или для преступной деятельности (размещение детской порнографии или незаконная продажа медикаментов, распространяемых по рецепту), в идеальном случае должны рассматриваться в течение нескольких часов. В случае атак "double flux"³ нарушителю достаточно нескольких минут задержки, чтобы обратить вектор атаки на другие зарегистрированные им доменные имена или доменные имена, к которым он получил несанкционированный доступ управления.

Рекомендации

ККБС рекомендует регистраторам и реселлерам участвовать в расследовании и борьбе с нарушениями и преступной деятельности в случаях, когда нарушители используют расширение доменного имени и регистрационные услуги. Организации ОПРИ рекомендуется учитывать следующее и предпринимать соответствующие действия.

1. Каждый регистратор должен предоставить канал связи для борьбы с нарушениями.
 - Этот канал связи по борьбе с нарушениями должен быстро и эффективно реагировать на запросы. Канал связи по борьбе с нарушениями должен быстро отвечать на вызовы по телефону или электронной почте; персонал, занимающийся рассмотрением нарушений, должен обладать достаточными полномочиями для эффективной работы и знать четко очерченный набор действий. Организации ОПРИ следует учитывать критерии доступности персонала по борьбе с нарушениями (напр., 24x7 или обычные рабочие часы) и среднее время ответа на жалобу. Информация о методе определения соответствия этим критериям должна быть предоставлена корпорации ICANN и регистраторам.
 - Регистраторы должны предоставлять четкую процедуру отслеживания жалоб о нарушениях с возможностью учета (напр., систему выдачи билетов или иную аналогичную систему). Организации ОПРИ следует вывести методы измерения производительности регистраторов и их соответствие требованиям.

³ См. документ SAC 025, "Хостинг Fast Flux и DNS", <http://www.icann.org/committees/security/sac025.pdf>

Канал связи регистратора для борьбы с нарушениями

2. Регистраторы должны публиковать контактную информацию лиц, занимающихся борьбой с нарушениями.
 - На веб-сайте регистратора, записанного в графе спонсирующего регистратора базы данных "Кто есть кто" (Whois), должна быть постоянно указана контактная информация для жалоб о нарушениях. ККБС рекомендует регистраторам, в целях обеспечения удобного (автоматического и быстрого) поиска соответствующей страницы членами сообщества, принять унифицированный формат именовании страниц, например, <http://www.<регистратор>.<ДВУ>/abuse.html>.
 - Регистраторы обязаны предоставить корпорации ICANN контактную информацию для борьбы с нарушениями, и ICANN опубликует эту информацию на странице <http://www.internic.net/regist.html>.
3. Информация о канале связи по борьбе с нарушениями, публикуемая регистратором, должна совпадать с контактной информацией, предоставленной в дополнении к Разделу 3.16 Договора об аккредитации регистратора. Все средства связи (телефон, адрес электронной почты и почтовый адрес) должны относиться к лицам или организациям, имеющим полномочия для рассмотрения жалоб о нарушениях; в частности, не допускается намеренное отклонение почтовых или электронных запросов лицами, чьи контактные сведения указаны.
 - Организация ККБС должна обозначить требования к контактной информации для борьбы с нарушениями, а также способ и место ее публикации. ОПРИ рекомендует регистраторам обратиться к документу RFC 2142, "Имена почтовых ящиков для обычных услуг, ролей и функций", и применять описанные в нем соглашения об именовании.
 - Канал связи по борьбе с нарушениями должен иметь унифицированный машиночитаемый формат. ОПРИ выносит решение, следует ли использовать один или все описанные варианты публикации.
4. Корпорация ICANN и регистраторы должны совместно с членами сообщества определять соответствующие меры защиты от ложных заявлений о нарушениях. Совместно с сообществами регистраторов и пользователей следует выработать определение понятия "нарушение" и меры защиты от ложных заявлений. Аналогичным образом, совместно с сообществами регистраторов и пользователей необходимо выработать критерии по скорости реагирования на жалобы. Эта деятельность должна осуществляться организацией ОПРИ в рамках всестороннего исследования нарушений, связанных с регистрацией доменных имен.
5. Корпорация ICANN должна периодически (не реже одного раза в год) проверять правильность указанной контактной информации.

Канал связи регистратора для борьбы с нарушениями

ККБС полагает, что наивысшее качество обслуживания сообщества достигается при наличии контактной информации регистраторов и реселлеров в удобном доступе и что наиболее целесообразным способом предоставления такой информации является единый список или база данных с возможностью поиска. Единый архив данных, поддерживаемый корпорацией ICANN, обеспечивает ей возможность быстро проверять точность и полноту контактной информации и предоставлять сообществу зримое подтверждение того, что корпорация ICANN и аккредитованные ею регистраторы стремятся предоставлять открытые и эффективные средства связи для общих запросов, а также для заявлений о нарушениях.

Эти рекомендации, в первую очередь, относятся к рДВУ и регистраторам, аккредитованным корпорацией ICANN. ККБС отмечает, что несмотря на уникальность структуры, договоров и соглашений с регистраторами для каждого ДВУ с кодом страны, желателен унифицированный подход к рассмотрению нарушений и предоставлению доступа к соответствующей контактной информации по всем ДВУ. Комитет ККБС предлагает ДВУ с кодами стран воспользоваться его опытом в обработке жалоб о нарушениях и сотрудничать с корпорацией ICANN с целью публикации контактной информации для борьбы с нарушениями и последовательного проведения соответствующих мер. Комитет ККБС готов к сотрудничеству с ОПРИ и ОПНИ в целях дальнейшей проработки этих вопросов.