
19 августа 2009 г.

**SAC 40: МЕРЫ ПО ЗАЩИТЕ УСЛУГ ПО
РЕГИСТРАЦИИ ДОМЕНОВ ОТ
НЕПРАВМОЧНОГО ИЛИ НЕДОПУСТИМОГО
ИСПОЛЬЗОВАНИЯ**

Отчет Консультативного комитета
по безопасности и стабильности
ICANN
(SSAC)

Введение

Этот отчет подготовлен Консультативным комитетом по безопасности и стабильности (SSAC) и содержит описание мер по защите регистрационных услуг от неправомерного использования. SSAC консультирует сообщество и Совет директоров ICANN по вопросам, связанным с безопасностью и целостностью систем распределения имен и адресов Интернета. К таким вопросам относятся эксплуатационные вопросы (например, вопросы, относящиеся к правильной и надежной работе системы корневых имен), административные вопросы (например, вопросы, относящиеся к распределению и назначению интернет-адресов) и регистрационные вопросы (например, вопросы, связанные с услугами реестров и регистраторов, такими, как WHOIS). SSAC занимается постоянной оценкой угроз и анализом рисков для служб распределения имен и адресов Интернета с целью определения источников основных угроз стабильности и безопасности, и предоставляет соответствующие рекомендации сообществу ICANN. SSAC не обладает полномочиями регламентировать, обеспечивать соблюдение или выносить судебное решение. Эти функции принадлежат другим органам, и содержащиеся здесь сведения и должны рассматриваться по существу дела.

Имена авторов этого отчета, ссылки на биографии членов комитета и заявления о сферах их интересов, а также возражения членов комитета, касающиеся результатов или рекомендаций этого отчета, содержатся в конце отчета.

Предисловие

Атаки, направленные на учетные записи регистрации доменных имен, и злонамеренное изменение конфигурации системы доменных имен (DNS) представляют собой опасные нарушения системы безопасности. Инциденты, произошедшие в течение последних нескольких лет, демонстрируют, что DNS и учетные записи регистрации доменов продолжают оставаться привлекательной мишенью для злоумышленников. Деятельность, *даже временная*, возникающая в результате несанкционированного изменения информации, связанной с регистрацией доменного имени, включая злонамеренное изменение информации о конфигурации DNS с целью использования DNS для перенаправления трафика в пункты, отличные от заданного узла, может привести к серьезному нарушению бизнес-операций и причинить финансовый и репутационный ущерб.

Перехваты учетных записей регистрации доменного имени и служб разрешения имен не являются новыми векторами атак. В предыдущих отчетах и информационных сообщениях Консультативный комитет по безопасности и стабильности ICANN (SSAC) рассматривал аспекты, оказывающие влияние на регистрацию доменных имен и эксплуатацию DNS с точки зрения пользователя (заказчика регистратора, т.е. владельца регистрации). Мы идентифицировали ситуации, в которых владельцы регистрации не предприняли достаточных мер для защиты доменных имен (например, не продлевали регистрацию или не сохраняли точных контактных данных). Мы рекомендовали меры, которые должны были предпринять владельцы регистрации для защиты своего бизнеса и оперативных интересов, в отношении зарегистрированных и управляемых ими доменных имен.

В настоящем отчете содержатся сведения о последних инцидентах, включающих несанкционированный доступ к учетным записям регистрации доменов. Целью упоминания подобных событий не является попытка поставить в неудобное положение или раскритиковать регистраторов, реселлеров *или* владельцев регистрации. Мы делаем это, поскольку анализ нарушений системы безопасности всегда вскрывает *что-либо*, что могла сделать каждая из сторон для предотвращения этого события или его последствий.

В настоящем отчете мы сосредоточиваем внимание на определенных значимых инцидентах, включающих учетные записи регистрации доменных имен, чтобы определить, существуют ли общие причины событий, которые могут подсказать действия, способные предотвратить определенные угрозы или смягчить их последствия. В отчете инциденты проанализированы достаточно подробно, чтобы определить, как были дискредитированы учетные записи, какие действия предпринимали злоумышленники после получения контроля над учетной записью, а также их последствия. Описания взяты из новостей и статей, открытых для публичного доступа. Эта информация была дополнена сведениями, полученными из бесед с регистраторами и их клиентами, которые подверглись нападению. Мы намеренно опускаем сведения, которые были определены пострадавшими сторонами как конфиденциальные.

В отчете представлены меры безопасности, используемые в других бизнес-сегментах Интернета (например, в финансовых, среди торговцев товарами длительного пользования) для защиты потребителей от аналогичных угроз. В отчете описываются действия, которые регистраторы могут предпринимать совместно с заказчиками, чтобы вместе защитить зарегистрированные домены от неправомерного использования, и обсуждаются методы повышения информированности владельцев регистраций о факторах риска, связанных даже с временной потерей контроля над доменными именами и связанными конфигурациями DNS. Хотя определенные регистраторы действительно отличаются от других, предлагая услуги высокого уровня качества, данный отчет преследует своей целью оказание помощи как можно большему количеству регистраторов в понимании того, какие существуют возможности обеспечения дополнительной защиты от атак, направленных на учетные записи регистрации доменов. Целью отчета является также разъяснение регистраторам того факта, что усиление мер безопасности при регистрации является одним из способов получения преимуществ перед конкурентами на рынке.

Что послужило причиной данной работы?

За последний год произошло несколько серьезных случаев несанкционированного доступа к учетным записям регистрации доменов. Все атаки обладали особенностями, сходными с теми, которые послужили причиной предшествующих исследований SSAC, посвященных перехвату доменных имен¹ и непредвиденным последствиям, связанным с невозобновлением доменных имен.^{2,3} Отдельные инциденты представляют собой злонамеренные акты, направленные против персонала регистраторов и регистрационных служб (например, веб-инструментов управления учетными записями доменов). Другие инциденты используют социотехнику, а также повседневную и ожидаемую переписку регистратора и его заказчиков.⁴

SSAC рассмотрел целый ряд инцидентов, произошедших с мая 2008 г. по апрель 2009 г. На основании этого рассмотрения мы определили уязвимые места, а также используемые политики и действия (деловые и оперативные), чтобы определить, имеются ли общие особенности. В ходе анализа этих инцидентов мы отметили следующее.

- (1) Многие организации имеют учетные записи регистрации доменного имени, которые содержат ценные или бизнес-критичные имена, доменные имена, которые могут быть настолько же ценными для организации, как и любые материальные ресурсы, товарный знак или интеллектуальная собственность, которой владеет организация.
- (2) Многие поставщики регистрационных услуг работают с услугами, ориентированными на потребителей, т.е. регистрационные услуги в высокой степени автоматизированы и сосредоточены на обслуживании очень большого количества владельцев регистраций с высокими показателями транзакций. Автоматизация имеет чрезвычайно важное значение в любой области бизнеса, где предпринимается попытка предоставления своевременных и масштабируемых услуг. В ходе исследования мы выяснили, что злоумышленники ознакомились с поведением владельцев регистраций и использовали отдельные аспекты автоматизации; например, зная о том, что электронная почта является предпочтительным способом уведомления владельцев регистраций об изменениях в контрактах, настройках,

¹ SAC007, Отчет о перехватах доменных имен,
<http://www.icann.org/announcements/hijacking-report-12jul05.pdf>

² SAC011, Проблемы, вызванные невозобновлением доменного имени, связанного с сервером имен DNS,
<http://www.icann.org/committees/security/renewal-nameserver-07jul06.pdf>

³ SAC010, Замечания о возобновлении для владельцев регистрации доменных имен,
<http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf>

⁴ SAC028, Информационное сообщение, касающееся противодействия фишинговым атакам по имитации регистраторов (26 мая 2008 г.),
<http://www.icann.org/committees/security/sac028.pdf>

о возобновлениях и т.д., злоумышленники часто пытаются помешать доставке на адреса электронной почты, изменяя конфигурацию DNS.

- (3) В рассмотренных нами инцидентах жертвами часто оказывались заказчики, имеющие критические для бизнеса учетные записи доменов, управление которыми осуществлялось поставщиками регистрационных услуг с ориентацией на потребителей. В отдельных случаях заказчики неадекватно оценивали риск, связанный с возможной утратой контроля или доступа к учетной записи регистрации их домена, до тех пор пока не оказывались жертвами; в других случаях внутренние политики и мониторинг перед инцидентом оказывались недостаточными для обнаружения или блокировки атаки.

Судя по размерам и бизнес-репутации, отдельные жертвы, казалось бы, должны быть достаточно осведомлены об управлении внутренней безопасностью и факторами рисками, чтобы адекватно оценить номинальную стоимость своих доменных имен, однако же не включили доменные имена в анализ риска. Другие жертвы, в особенности малые и средние предприятия или физические лица не вполне осознавали важность своих доменов, пока не возникли проблемы. Это согласуется с поведением в отношении других факторов риска. Во многих ситуациях организация может адекватно оценить стоимость или критичность для бизнеса того или иного ресурса, но при этом не предпринять соответствующих мер для защиты этого ресурса от угроз, до тех пор пока не возникнут проблемы.

С точки зрения безопасности, владельцы регистраций, считающие свои доменные имена критически важными ресурсами, должны сделать безопасность одним из решающих критериев при выборе поставщика регистрационных услуг. В результате анализа инцидентов SSAC обнаружил, что владельцы регистрации либо не осознают всего ассортимента услуг по обеспечению безопасности, предлагаемых поставщиками регистрационных услуг, либо они не принимают во внимание, что *существует* целый ассортимент услуг по обеспечению безопасности. Один владелец регистрации признался SSAC, что владельцы регистраций полагают, что все регистрационные услуги похожи одна на другую, и сделал вывод, что, поскольку все регистраторы продают один и тот же продукт из одних и тех же реестров, предлагаемые ими меры безопасности также предположительно одинаковы. Инциденты, описываемые нами в следующих разделах, помогли SSAC сделать вывод, что за пределами сообщества доменных имен не существует четкого понимания различий между поставщиками регистрационных услуг.

Атаки, направленные на учетные записи регистрации доменных имен

Хотя составление исчерпывающего списка событий, связанного с данной темой, не входит в задачи данного отчета, мы представим сводные сведения об определенных серьезных атаках, направленных на учетные записи регистрации доменных имен, чтобы привести контекст для дальнейшего обсуждения и анализа. В этих сводных сведениях содержится информация из открытых источников, кроме того, SSAC также проводил консультации с регистраторами, участвовавшими в инцидентах, а также с организациями, ставшими жертвами злоумышленников, и благодарит их за сотрудничество.

Comcast (май 2008)

Comcast является крупнейшим поставщиком услуг кабельного телевидения, вторым по значимости поставщиком интернет-услуг и находится среди крупнейших поставщиков услуг телефонной связи в США.⁵ На момент инцидента компания Comcast зарегистрировала около 200 доменов при посредничестве Network Solutions, Inc.⁶ 28 мая 2008 г. злоумышленники получили доступ к регистрационной учетной записи Comcast в Network Solutions. Сначала злоумышленники злонамеренно изменили определенные контактные данные, предположительно для получения известности.⁷ Персонал Comcast получил уведомление по электронной почте об этих изменениях и восстановил правильные сведения.

Злоумышленники утверждают, что позвонили администратору Comcast и объяснили, в чем состоят уязвимые места и что именно они использовали для атаки. Злоумышленники утверждают, что использовали сочетание социальной инженерии и технический взлом для получения доступа к учетной записи регистрации домена.⁸ Network Solutions заявила, что не было нарушения системы безопасности или социотехнического воздействия на персонал, а изменения DNS были сделаны кем-то, кто располагал учетными сведениями пользователя для входа в систему.⁹ В статье в журнале *Wired Magazine* злоумышленники утверждали, что менеджер Comcast "поднял их на смех и повесил трубку".¹⁰ Злоумышленники во второй раз осуществили доступ к учетной записи. На этот раз они изменили DNS-конфигурацию домена comcast.net и перенаправили трафик на искаженный веб-сайт, размещенный на взломанных ими серверах. Тем не менее, персонал Comcast не получил уведомления об изменениях по электронной почте от Network Solutions. В контактной информации технического специалиста и администратора в регистрационной записи домена использовались адреса электронной почты, отведенные зарегистрированным доменам Comcast. Изменив DNS-конфигурацию, злоумышленники помешали персоналу Comcast получить уведомления по электронной почте об изменениях учетной записи: они просто не могли быть доставлены. Атака оказалась эффективной и попала на первые полосы газет во всем мире. Выдержка из *Wired Magazine*: "Атака началась около 23:00 по восточному времени, и злоумышленники владели Comcast.net до 4:00 или 5:00. Даже когда Comcast восстановил контроль, прошло еще несколько часов, пока изменения были полностью внедрены в DNS, в результате чего отдельные пользователи оставались без доступа к электронной почте до 11:30 в четверг". В статье в *The Register* 29 мая 2008 г. отмечается, что "атака продемонстрировала, что взлом

⁵ Статья о Comcast: en.wikipedia.org/wiki/Comcast

⁶ Домен Comcast.net перехвачен в Network Solutions, <http://www.domainnamenews.com/featured/comcastnet-domain-hijacked-at-network-solutions/1619>

⁷ Как был взломан Comcast.net?, <http://blogs.zdnet.com/security/?p=1224>

⁸ Перехват имени Comcast.net, <http://www.internetidentity.com/2008/June-2008.html>

⁹ Проблема с доступом к учетной записи Comcast — разъяснение, <http://blog.networksolutions.com/2008/comcast-account-access-issue-clarification/>

¹⁰ Похитители Comcast утверждают, что предупреждали компанию, <http://blog.wired.com/27bstroke6/2008/05/comcast-hijacke.html>

Данный документ переведен с английского языка в целях расширения аудитории его читателей. Несмотря на усилия, предпринятые некоммерческой организацией ICANN в отношении проверки точности перевода, единственной официальной версией данного документа, имеющей силу, является англоязычная версия, поскольку английский является рабочим языком ICANN. Исходный документ на английском языке находится по адресу: <http://www.icann.org/committees/security/sac040.pdf>.

старомодных учетных записей достаточен для изменения значительных объемов веб-трафика".¹¹

CheckFree (декабрь 2008 г.)

CheckFree (теперь FIServ) является ведущим международным поставщиком систем информационного менеджмента и электронной коммерции для финансовых фирм.¹² 2 декабря 2008 г. злоумышленник захватил контроль над учетной записью регистрации домена CheckFree в Network Solutions.¹³ Злоумышленник модифицировал DNS-конфигурацию нескольких доменов, включая checkfree.com и mycheckfree.com. Пользователи, пытавшиеся получить доступ к учетной записи, чтобы воспользоваться услугами электронных платежей через Интернет, были перенаправлены на мошеннический сервер на Украине, где была осуществлена попытка установить вредоносный код, содержащий средство атаки Adobe Reader.¹⁴ CheckFree восстановил правильную DNS-конфигурацию в течение восьми часов после начала атаки, но, как и в случае аналогичных инцидентов, внедрение изменений в пределах международной DNS-инфраструктуры заняло на много часов больше.¹⁵

В блоге "Security Fix" газеты *Washington Post* отмечалось, что злоумышленник получил доступ к учетной записи с использованием верных учетных сведений. В той же статье Network Solutions подчеркивала, что злоумышленник не взламывал их системы, чтобы получить учетные сведения.¹⁶ Остается неясным (или невыясненным), каким именно образом злоумышленник получил учетные данные для доступа к учетной записи.

ICANN, Photobucket, RedTube (июнь 2008)

26 июня 2008 г. ICANN сама стала жертвой группы злоумышленников, которые получили несанкционированный доступ к учетной записи регистрации домена ICANN на Register.com. Согласно пресс-релизу ICANN, атака была "сложной и использовала как социальные, так и технические технологии".¹⁷ По словам ИТ-руководителя ICANN, злоумышленники изменили DNS-конфигурацию нескольких доменов — icann.net, iana-servers.com, icann.com, internetassignednumbersauthority.com и iana.com — так, что трафик посетителей перенаправлялся на искаженный веб-сайт, размещенный на бесплатных учетных записях,

¹¹ Безумные хакеры похищают ключи Comcast.net, чтобы прокатиться, http://www.theregister.co.uk/2008/05/29/comcast_domain_hijacked/

¹² FIServ, <http://en.wikipedia.org/wiki/Fiserv>

¹³ DNS-атака перехватывает платежный веб-сайт, <http://www.techworld.com/security/news/index.cfm?newsid=107959>

¹⁴ Фишинговая атака Network Solutions предшествовала захвату домена CheckFree, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122722>

¹⁵ <http://www.internetidentity.com/2008/Nov-Dec-2008-FIN.html#cf>

¹⁶ Более глубокие сведения об атаке на CheckFree, http://voices.washingtonpost.com/securityfix/2008/12/digging_deeper_into_the_checkf.html

¹⁷ Ответ ICANN на последние угрозы безопасности, <http://www.icann.org/en/announcements/announcement-03jul08-en.htm>

управление которыми осуществляется Atspace.com. Предположения о том, что атака имела политические причины, было основано на сроках инцидента (начало парижского совещания ICANN, где проходило открытое обсуждение новых оДВУ), а также на самом искаженном сообщении. ИТ-персонал обнаружил изменения DNS, и Register.com восстановил правильную конфигурацию вскоре после уведомления от ICANN. Однако, как и в инциденте с Comcast, вредоносная информация о конфигурации DNS сохранялась в международной системе DNS еще в течение 24–48 часов,¹⁸ пока восстанавливалась корректная информация.

Группа хакеров, которая приняла на себя ответственность за атаку на ICANN, использовала аналогичную тактику и того же поставщика бесплатных услуг по размещению веб-узлов в ходе последующих атак. Photobucket представляет собой веб-сайт, предоставляющий услуги по размещению изображений, видеоматериалов, слайд-шоу и фотографий, приобретенный компанией Fox Interactive Media в 2007 г.¹⁹ 18 июня 2008 г. та же группа взломщиков приняла на себя ответственность за атаку на Photobucket, которая привела к перебоям в предоставлении услуг пользователям Photobucket.²⁰ Эта же группа предприняла еще одну атаку, направленную на искажение внешнего вида веб-сайта, 7 февраля в отношении сайта RedTube, содержащего материалы для взрослых.^{21, 22}

DomainZ (апрель 2009)

DomainZ (Domainz.net.nz) представляет собой новозеландский филиал компании MelbourneIT и выступает в качестве регистратора. 21 апреля 2009 г. лица, в поисках известности, предприняли атаку с внедрением SQL на страницу извлечения паролей на DomainZ для сбора учетных сведений нескольких солидных владельцев регистраций, включая Coca-Cola, Fanta, F-secure, HSBC, Microsoft, Sony и Xerox. Злоумышленники модифицировали записи DNS-конфигурации доменов, зарегистрированных в .CO.NZ, чтобы они указывали на серверы имен, зарегистрированные в домене .INFO (turkguvenligi.info). На этих серверах была размещена несанкционированная информация о зонах, в соответствии с которой выполнялось разрешение взломанных доменов в искаженные веб-сайты злоумышленников. Определенная часть трафика посетителей перенаправлялась на вредоносные веб-сайты, целью которых была атака на брэнд (например, Microsoft), другой трафик перенаправлялся на страницы, содержащие материалы с политическим протестом.

¹⁸ Турецкие преступники перехватывают веб-сайты ICANN, http://news.cnet.com/8301-10789_3-9980713-57.html

¹⁹ Photobucket, <http://en.wikipedia.org/wiki/Photobucket>

²⁰ DNS-записи Photobucket перехвачены группой турецких взломщиков, <http://blogs.zdnet.com/security/?p=1285>

²¹ Популярный порносайт атакован ханжами, <http://www.securecomputing.net.au/News/102818,popular-porn-site-hacked-by-prudes.aspx>

²² Турецкие хакеры атакуют самый популярный порносайт, <http://www.darkreading.com/security/perimeter/showArticle.jhtml;jsessionid=FV31FLACFRJQYQSNLPSKH0CJUNN2JVN?articleID=208803672&subSection=Security>

Что показали эти инциденты?

Схожесть методов атаки на Comcast, ICANN, Photobucket и RedTube иллюстрирует, что взломщики регистрационных учетных записей аналогично используют интернет, передачу файлов и другие интернет-приложения следующим образом: после того как то или иное уязвимое место успешно использовалось, злоумышленники продолжают использовать вредоносный код и сканируют объекты атаки с целью обнаружения тех же или аналогичных уязвимых мест.

На основании анализа данных инцидентов SSAC отмечает следующее.

Для отдельных регистраторов:

1. Все, что необходимо злоумышленнику для получения контроля над всем набором доменных имен организации (и для затруднения авторизованного доступа к этому набору) — это учетная запись пользователя и пароль.
2. Злоумышленники могут лишь предположить, выудить эти данные или использовать технологии социальной инженерии для их получения у единственного контакта, чтобы получить контроль над учетной записью регистрации домена.
3. Злоумышленники сканируют регистрационные учетные записи доменов и административные порталы на предмет обнаружения уязвимых мест (например, внедрение SQL). Успешный вредоносный код или уязвимый код приложения могут привести к раскрытию учетных сведений для многих учетных записей доменов.
4. Электронная почта является предпочтительным и часто единственным способом, которым некоторые регистраторы пытаются уведомить владельца регистрации о деятельности в области учетной записи. (Другие методы связи мы обсудим в последующих разделах).
5. Злоумышленники могут заблокировать уведомления по электронной почте, направляемые владельцам регистраций, изменяя информацию о DNS-конфигурации таким образом, что уведомления по электронной почте не доходят ни до одного получателя в тех доменах, которые злоумышленник контролирует через взломанную учетную запись (например, указанные владельцем регистрации адреса электронной почты административного или технического специалиста, размещенные на домене).
6. Доступ и возможность изменения контактной информации и DNS-конфигурации для всех доменов в регистрационной учетной записи обычно предоставляется через единственную учетную запись пользователя и пароль.
7. Даже если несанкционированное изменение информации DNS обнаруживается быстро, процесс восстановления DNS-информации для исправления вредоносной конфигурации может занять длительное время, что вытекает из распределенной природы DNS и связано со значениями времени жизни (TTL).

Заказчики не знакомы с мерами по защите регистраций

Отдельные регистраторы предпринимают значительные усилия по защите своего бизнеса и своих заказчиков. Они применяют передовой опыт для защиты веб-приложений, серверов имен и хост-серверов. Они осуществляют мониторинг систем и учетных записей на предмет подозрительной деятельности. Служба поддержки регистраторов эффективно реагирует на злоупотребления или жалобы на преступную активность. Тем не менее, в такой широкой области, как услуги регистрации доменных имен (как и с любыми электронными торговцами или интернет-бизнесом), отдельные регистраторы неизбежно оказываются уязвимыми для известных направлений атак. Другие, даже самые лучшие, могут оказаться уязвимыми для атак, которые не рассматривались во время аудита вопросов безопасности или же вообще никогда еще не встречались.

На основании анализа инцидентов, рассмотренных в данном отчете (и других аналогичных инцидентов, приведенных в документе SAC012 и произошедших с момента его публикации), следует очевидный вывод, что процесс регистрации был и продолжает использоваться злоумышленниками. С учетом масштабов и разнородности отрасли в этом нет ничего удивительного. Регистраторы были и продолжают оставаться мишенями для злоумышленников. *Так же как клиенты финансовых учреждений могут оказаться жертвами нападения на банковский интернет-портал, регистраторы доменных имен могут оказаться жертвами нападений на веб-страницы управления доменами регистраторов.*

В обязанности прежде всего владельца регистрации входит оценка риска нападения на доменное имя и DNS-конфигурацию и выбор поставщика регистрационных услуг, который бы снизил для владельца регистрации риск подвергнуться атаке до приемлемого уровня. Тем не менее, регистраторы обычно не привлекают внимания к предлагаемым ими мерам безопасности, а поскольку способы сравнения служб безопасности регистраторов отсутствуют, клиенты могут ошибочно предположить, что все регистраторы одинаковы в отношении мер безопасности, и сделать неправильный или необдуманный выбор.

Регистраторы имеют различные целевые рынки и модели услуг

Имея это в виду, SSAC рассмотрел широкий массив услуг по регистрации доменных имен и определил, что регистрация доменных имен главным образом поддерживается двумя моделями услуг.

В одной популярной модели услуг регистрация доменного имени предлагается по ценам от средних до низких. Организация услуг в высокой степени автоматизирована и рассчитана на быстрое выполнение транзакций, в большом объеме, согласованным способом, в результате чего возможность человеческой ошибки часто сводится к минимуму. Переписка с заказчиками обычно осуществляется посредством сообщений электронной почты, которые доставляют уведомления или передают простые (часто пошаговые) инструкции, помогающие клиентам пройти через обязательные процедуры (например, ежегодный отчет WHOIS). Обычным делом являются автоматизированные отчеты о неисправностях через систему выдачи билетов. В целом, автоматизация играет большую роль, чем человеческое участие; в большинстве случаев об участии человека, как правило, просят заказчики, когда

автоматические процедуры выполняются не так, как ожидалось, или же когда у заказчика возникает проблема, которую не может разрешить автоматическая процедура, или он должен сообщить о каком-либо инциденте. Обычные, видимые меры безопасности для защиты учетных записей доменов и DNS-конфигурации от злоупотреблений обычно включают защищенный по протоколу защищенных сокетов (SSL) вход в учетную запись домена и управление набором доменов, уведомления по электронной почте, когда вносятся изменения в DNS или контактную информацию, связанную с учетной записью, услуги конфиденциальности (защищенные или делегированные услуги WHOIS, как обсуждалось в документе SAC023²³), а также защиту передачи доменов (блокировку регистраторов, авторизацию, подтверждение кода между теряющим и приобретающим регистратором).²⁴

В рамках второй модели регистрационных услуг предлагаются защитные меры, удовлетворяющие потребностям заказчиков, которые высоко ценят свои доменные имена, рассматривают доменные имена и интернет-присутствие как критически важные факторы или же понимают, что их бизнес или брэнд может оказаться мишенью для неправомерного использования или преступной деятельности. Эти заказчики в полной мере осознают вероятность угроз доменным именам и пытаются сократить или смягчить риск потери, ошибки конфигурации, изменения контактной информации или DNS-конфигурации, а также неправомерного использования их доменов; поэтому они собирают достаточно полные сведения для принятия информированного решения по выбору того или иного регистратора, который бы удовлетворял всем этим требованиям. Такие регистраторы предпринимают меры безопасности для защиты от невозобновления доменного имени заказчика в результате технической ошибки или недосмотра, для защиты заказчика от перехвата доменного имени в результате несанкционированного изменения регистрационных записей и для предотвращения несанкционированного, злонамеренного изменения DNS-конфигурации. Бизнес-модель для этих регистраторов сосредоточена на обработке индивидуальных транзакций с очень низкой вероятностью ошибки. Регистратор обслуживает заказчиков, уделяющих первостепенное внимание средствам защиты и готовых платить высокую цену за человеческую помощь (в частности, за помощь специалиста по учетным записям, который выделяется заказчику). Заказчики могут, например, в целях безопасности потребовать устного или письменного подтверждения от утвержденного заказчиком контактного лица, прежде чем производить какие-либо изменения и мониторинг в реальном времени DNS-конфигурации и служб разрешения имен.

Обычно перечисленные выше меры входят в более широкий пакет, который направлен на защиту прав брэнда. Меры по защите прав брэнда имеют своей целью снизить степень риска, включая возможность неправомерного использования товарных знаков (т.е. несанкционированное использование товарного знака или брэнда для привлечения пользователей Интернета к веб-сайту, не имеющему отношения к владельцу товарного знака

²³ SAC023, Является ли сервис WHOIS источником адресов электронной почты для спамеров?
<http://www.icann.org/en/committees/security/sac023.pdf>

²⁴ Отдельные регистраторы внедряют меры защиты внутренних, критичных для бизнеса систем, процессов и баз данных. Они обычно невидимы для клиентов регистратора.

Данный документ переведен с английского языка в целях расширения аудитории его читателей. Несмотря на усилия, предпринятые некоммерческой организацией ICANN в отношении проверки точности перевода, единственной официальной версией данного документа, имеющей силу, является англоязычная версия, поскольку английский является рабочим языком ICANN. Исходный документ на английском языке находится по адресу: <<http://www.icann.org/committees/security/sac040.pdf>>.

или брэнда), регистрацию доменов, направленную на владельца брэнда (визуально похожие, гомографические домены, используемые для фишинговых или мошеннических атак), доход от изменения маршрута трафика (попытки регистрации доменов от имени заказчика, которые уже зарегистрированы другими сторонами, в случае если они снова станут доступными), а также оборонительная регистрация (регистрация товарного знака или имени на всех доменах высшего уровня).

Кто нуждается в защите от перехвата учетных записей доменов и DNS?

Действенные меры по защите от злонамеренного изменения информации, касающейся учетной записи домена или конфигурации DNS, обычно знакомы и приветствуются организациями, которые вкладывают значительные средства в наборы доменов или права брэнда, а также имеют средства и желание платить за защиту своих брэндов. Однако *владельцы регистраций не должны полагать, что только компании с брэндами или имеющие интеллектуальную собственность нуждаются в защите от перехватов учетных записей доменов или от злонамеренного изменения информации или конфигурации DNS.* Многие организации, жизненно зависимые от присутствия в Интернете, могут не использовать доменные имена, связанные с брэндами. Другие организации могут вести дела под любым из зарегистрированных доменных имен. Такие организации, тем не менее, будут испытывать ущерб или финансовые потери, если имена, которые они назначат своим интернет-услугам, электронной почте и другим услугам, не будут разрешаться в адреса интернет-протокола (IP), где эти организации размещают свои услуги.

С учетом того, что определенные организации *получат* преимущества благодаря выбору регистрационных услуг, которые значительно снизят степень риска, связанную с потерей доменного имени или со злонамеренным изменением информации или DNS-конфигурации, мы попытались определить возможные причины, по которым организации могут выбирать регистраторов, не учитывая предлагаемые ими меры безопасности. Некоторые из этих возможных причин следующие.

Кажущаяся стоимость: в отдельных случаях организация предполагает или делает ошибочный вывод, что стоимость регистрации домена посредством регистратора, предлагающего действенные меры защиты от перехвата учетной записи домена и DNS, чересчур высока.

Информированность: определенные заказчики с удовольствием заплатили бы за действенные меры по защите от перехвата учетной записи домена и DNS, однако просто не знают, что такие услуги существуют.

Ограниченность источников информации: в некоторых случаях, пользуясь ограниченными источниками информации, организация делает ошибочный вывод, что все регистраторы предлагают одинаковые меры защиты.

"Ваш пакет услуг не подходит для моей организации": в некоторых случаях организация с удовольствием заплатила бы за действенные меры защиты от перехвата учетной записи домена и DNS, но не хочет или не может оплачивать услуги, которые отдельные регистраторы (по ощущениям) включают в пакет, например действенные меры защиты плюс защита прав брэнда.

В этом контексте заслуживают рассмотрения еще несколько вопросов.

Заинтересованы ли в действенных мерах по защите регистрации только те организации, которые стремятся защитить свои брэнды?

Нет. Многие организации должны балансировать между стремлением защитить свой брэнд и интернет-присутствие и стоимостью защитных мер. Усиленные меры по защите регистрации часто предлагаются как дополнение к защите прав брэнда. Усиленные меры по защите регистрации, возможно, предлагаемые в дополнение к базовым регистрационным услугам — как дополнительная услуга или услуга "за вознаграждение" — могут сделать желанные меры безопасности доступными для организаций, которые стремятся вкладывать средства в меры безопасности, чтобы уменьшить потенциальную возможность потери доступности в результате неправомерного или неправомерного использования.

Должны ли организации, не имеющие стремлений защиты брэндов, рассматривать доменные имена при оценке рисков и управлении ресурсами?

Да. В отчетах SSAC объяснены отрицательные последствия, с которыми сталкиваются владельцы регистраций при перехвате доменных имен, включая финансовые убытки, запутанность и ущерб репутации.²⁵ В отчетах SSAC также объясняются проблемы, вызванные невозобновлением доменных имен, и проблемы, вызванные невозобновлением доменного имени, связанного с сервером имен DNS.²⁶ В частности, SSAC отмечает в документе SAC010, что "доменные имена должны рассматриваться как ресурсы, имеющие рыночную стоимость посредством либо продажи через брокера,

либо непосредственной продажи, или же как средства, генерирующие постоянный доход", а также, что "владельцы регистраций, не возобновляющие зарегистрированные доменные имена, добровольно или непреднамеренно, должны иметь в виду, что каждое доменное имя представляет для кого-то потенциальную ценность — и новые владельцы регистраций могут

²⁵ SAC007: Отчет о перехватах доменных имен (12 июля 2005 г.) <http://www.icann.org/announcements/hijacking-report-12jul05.pdf>

²⁶ SAC011: Проблемы, вызванные невозобновлением доменного имени, связанного с сервером имен DNS (7 июля 2006 г.) <http://www.icann.org/en/committees/security/renewal-nameserver-07jul06.pdf>

Данный документ переведен с английского языка в целях расширения аудитории его читателей. Несмотря на усилия, предпринятые некоммерческой организацией ICANN в отношении проверки точности перевода, единственной официальной версией данного документа, имеющей силу, является англоязычная версия, поскольку английский является рабочим языком ICANN. Исходный документ на английском языке находится по адресу: <http://www.icann.org/committees/security/sac040.pdf>.

использовать ставшее недействительным имя домена таким образом, который может оказаться пагубным для предшествующего владельца регистрации".²⁷

Какие защитные меры могут быть предложены организациям, рассматривающим доменные имена как ресурсы, чтобы оказать им помощь в управлении рисками и смягчении последствий угроз их капиталовложениям и зависимости от доменных имен?

Определенные меры, используемые в других бизнес-сегментах Интернета (например, в финансовых, среди торговцев товарами длительного пользования), могут эффективно и практично использоваться для защиты регистрационных услуг. Прежде чем рассматривать конкретные меры и ради блага самих владельцев регистраций, следует еще раз вспомнить основные принципы: как конкретно структуры управления ресурсами, снабжением и рисками, используемые в крупных организациях, применяются к регистрации доменных имен? Почему следует считать ресурсом регистрацию доменного имени?

В предшествующих отчетах SSAC объяснялось, что доменное имя представляет собой отличительную черту, по которой некий объект — торговец, финансовое или образовательное учреждение, коммерческую или некоммерческую организацию, физическое лицо или продукт — известен или ведет бизнес в Интернете. Это может быть то же самое имя, которое корпорация регистрирует в качестве официального наименования, под которым она ведет свою деятельность, имя знаменитости, автора, политического лица или другой личности. Как физические, так и юридические лица рассматривают имена (бренды, знаки обслуживания, товарные знаки) в физическом мире как ресурсы и предпринимают меры по их защите от злоупотреблений (свидетельства о регистрации корпораций, патенты, авторские права и т.д.). Доменное имя часто представляет собой то же самое, что и бренд организации, товарный знак или знак обслуживания, и поэтому владельцы регистраций должны принять меры по защите таких имен не только посредством их регистрации, но и защитив их от неправомерного использования.

Регистрация доменного имени обеспечивает уникальность домена в международном масштабе и связывает домен с владельцем регистрации, пока он продолжает уплачивать пошлину за возобновление регистрации и выполнять договорные обязательства (например, в отношении допустимого использования, точности регистрации). Оно поэтому эквивалентно другим дисциплинам сетевого управления, таким, как ресурс, риск и снабжение.

Доменные имена также представляют собой удобные для пользователя идентификаторы, которые могут быть разрешены с использованием DNS для определения интернет-адресов узлов, предоставляющих услуги для этого домена (веб, электронная почта, социальные сети, голос...). Операционная ценность домена — в частности, гарантия того, что разрешение имени обладает высокой доступностью и что имена в домене разрешаются должным образом — представляет собой огромную важность для большинства организаций.

²⁷ SAC010: SAC010, Замечания о возобновлении для владельцев регистрации доменных имен (29 июня 2006 г.), <http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf>

Данный документ переведен с английского языка в целях расширения аудитории его читателей. Несмотря на усилия, предпринятые некоммерческой организацией ICANN в отношении проверки точности перевода, единственной официальной версией данного документа, имеющей силу, является англоязычная версия, поскольку английский является рабочим языком ICANN. Исходный документ на английском языке находится по адресу: <<http://www.icann.org/committees/security/sac040.pdf>>.

Например, в контексте программы управления ресурсами и рисками возможно следующее:

- определить ценность ресурса (материального или нематериального);
- перечислить угрозы этому ресурсу (потеря, кража, неправомерное использование);
- определить, как может быть реализована эта угроза, т.е. определить, что делает доменное имя уязвимым для атаки или неправомерного использования;
- определить вероятность риска, которые представляет каждая угроза;
- определить способы снижения степени риска;
- определить стоимость снижения степени риска до приемлемого уровня;
- определить соответствующий бюджет и задействовать программу снижения степени риска.

Если доменное имя представляет собой ресурс, оно требует тех же мер, что и другие инвентарные, ценимые или секретные ресурсы. В этом свете управление регистрацией доменного имени обладает многими характеристиками управления развертыванием ресурсов в крупномасштабных сетях. Например, первичные операции в развертывании ресурсов и в регистрации доменного имени следующие: {добавить, удалить, изменить}. Передовой опыт, используемый в управлении развертыванием ресурсов, преследует целью гарантировать, что эти операции выполняются в должной последовательности, авторизованными сторонами, своевременно и с возможностью проверки, с низкой вероятностью недосмотров, вмешательств и ошибок. Подобный передовой опыт должен использоваться и в управлении регистрацией доменных имен, а поставщики услуг регистрации должны стремиться к его внедрению.

Меры безопасности, направленные на защиту регистрации доменных имен, должны иметь такое же важное значение для организации, как и меры безопасности, используемые организацией для защиты внутренних корпоративных сетей, удаленных баз данных и других ресурсов приложений, которые организация считает критически важными для бизнеса. Чтобы свести к минимуму вероятность недосмотров, вмешательств или ошибок в управлении регистрацией доменных имен, заказчики, рассматривающие регистрацию доменного имени как значимый ценный ресурс, должны стремиться к внедрению проверки подлинности, авторизации и аудиторских услуг, которые применяются в отношении других критически важных для бизнеса приложений. Некоторые из этих мер могут быть предприняты заказчиком. Другие могут быть включены в регистрационные услуги регистраторами, решившими, что предоставление дополнительных услуг по защите способствует получению ими преимуществ перед конкурентами на рынке. Более подробно это будет рассмотрено в следующих разделах.

Меры по предотвращению перехвата учетных записей доменных имен и DNS

В данном разделе описываются меры, предпринимаемые сегодня отдельными регистраторами в качестве составной части более широкого пакета услуг, часто в сочетании с защитой интернет-репутации (прав брэнда). Далее описываются услуги, которые могут предложить регистраторы и которые участники обсуждения инцидентов 2008 года с SSAC определили как желательные или необходимые. И наконец, будут рассмотрены мероприятия, проводимые крупными организациями для обеспечения безопасности доступа к удаленным приложениям, а также меры, которые предпринимают финансовые учреждения и организации, занимающиеся электронной торговлей, для защиты учетных записей клиентов. Эти меры могут предлагаться как дополнительные услуги или в составе пакета услуг и всегда способствуют укреплению безопасности учетной записи регистрации домена для заказчиков, которые готовы вкладывать средства в дополнительные меры безопасности с целью снижения степени риска неправомерного использования учетной записи домена. Регистраторам предлагается также рассмотреть, создаст ли внедрение этих мер для них дополнительные возможности и будет ли способствовать получению преимущества перед конкурентами на рынке.

Заказчики (владельцы регистраций) играют важнейшую роль в защите доменных имен. В данном разделе мы вкратце опишем определенные дополнительные меры, которые могут и должны предпринять заказчики, чтобы (а) защитить свою роль в рабочем процессе "регистратор-владелец регистрации", связанном с созданием регистрации домена и его возобновлением и (б) защитить процесс управления и изменения контактной и конфигурационной информации. Регистраторы могут рекомендовать такие меры в существующих или новых списках часто задаваемых вопросов или с использованием других средств тем заказчикам, которые владеют критически важными наборами доменов. Например, регистраторам предлагается ознакомить с этим отчетом заказчиков и убедить их изучить этот отчет и внедрить меры, которые они посчитают необходимыми для снижения степени тех рисков, которые, по их мнению, представляют наибольшую опасность для наборов их доменных имен.

SSAC полагает, что предложение услуг, связанных с защитой регистрации домена, обладает большим потенциалом для восприятия и может быть более исчерпывающим, чем сумма инициатив или независимая их реализация малыми и средними предприятиями. В этом утверждении мы основываемся на успешном использовании средств защиты, входящих в объединенную систему управления угрозами (UTM): системы безопасности, включающие межсетевой экран, средства борьбы со спамом, антивирусные программы и другие средства безопасности. Эти системы чаще применяются и пользуются большим успехом на рынке среди малых и средних предприятий, чем лучшие сочетания систем безопасности, предлагающие лишь одну меру безопасности. Мы полагаем, что предложение дополнительных услуг по обеспечению безопасности может оказаться настолько же успешным при регистрации доменов малыми и средними предприятиями, насколько успешной оказалась объединенная система управления угрозами.

Защита доступа к набору доменов

Меры, описанные в данном разделе, направлены на защиту от несанкционированного доступа к учетной записи доменного имени заказчика посредством веб-интерфейса или службы технической поддержки регистратора или реселлера или телефонной службы технической поддержки.

Проверка регистрации. Модель регистрации, оптимизированная для транзакций большого объема и быстрого развертывания доменных имен часто не оптимизирована для проверки того, является ли регистратор тем, за кого он себя выдает, и того, не совершается ли при оплате мошенничества или преступления. Исследования антифишинга,^{28:29} опыт борьбы с бот-сетями (Srizbi, Conficker) и атаки Fast Flux иллюстрируют, что учетные записи регистрации доменов являются и будут продолжать являться ключевым ресурсом для преступной деятельности. Проверка информации о канале связи, предпринимаемая владельцем регистрации при регистрации и при каждом изменении контактной информации, может сократить количество случаев выдачи себя за другое лицо и неправомерного использования доменов. Регистраторам предлагается рассмотреть возможность предложения проверки регистрации по электронной почте; регистрация домена осуществляется только в том случае, когда владелец регистрации подтверждает свой адрес электронной почты путем перехода по ссылке, встроенной в активационное сообщение, отправленное регистратором. В качестве дополнительной меры отдельные финансовые организации могут звонить по телефону, указанному заказчиком, а не пользоваться электронной почтой. Компания называет подтверждающий номер по телефону, а заказчик вводит его в веб-форму для активации учетной записи или авторизации транзакции. SSAC признает, что подобные меры приводят к задержкам в процессе регистрации и доставки продукта (регистрации и разрешения имени зарегистрированного доменного имени), однако регистраторам предлагается сравнить эти задержки с последствиями неправомерного использования не только в отношении заказчика, но и в отношении расширенного интернет-сообщества. Дополнительным преимуществом является то, что регистраторы, предпринимающие превентивные меры для защиты системы имен Интернета, приобретают положительную репутацию и обычно рекомендуются профессионалами в области безопасности и коллегами по бизнесу.

Усовершенствование систем проверки подлинности, основанных на паролях.

Основным средством проверки подлинности среди регистраторов является обычное имя пользователя и пароль. От регистраторов не требуется устанавливать минимальную длину, максимальный срок службы или проверку сложности пароля, который также может быть не защищен от грубых попыток угадывания посредством ограничения количества попыток неправильного ввода. Признанный передовой опыт свидетельствует о том, что эти меры должны присутствовать в любой системе проверки подлинности, основанной на паролях.

²⁸ Отчет APWG о тенденциях фишинга, 2-я часть 2008, http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf

²⁹ Глобальный обзор по фишингу: Использование доменных имен и тенденции в 2008 г. http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf

Данный документ переведен с английского языка в целях расширения аудитории его читателей. Несмотря на усилия, предпринятые некоммерческой организацией ICANN в отношении проверки точности перевода, единственной официальной версией данного документа, имеющей силу, является англоязычная версия, поскольку английский является рабочим языком ICANN. Исходный документ на английском языке находится по адресу: <<http://www.icann.org/committees/security/sac040.pdf>>.

Системная регистрация. Организации, занимающиеся электронной торговлей, и финансовые учреждения теперь дополняют системы, основанные на паролях, тем, что позволяют пользователю зарегистрировать персональный компьютер или IP-адрес, с которого он будет управлять учетной записью.

Многофакторная проверка подлинности Организации, занимающиеся электронной торговлей, финансовые учреждения и даже операторы интернет-игр (ролевых игр) предлагают клиентам возможность воспользоваться аппаратным ключом в качестве второго фактора аутентификации для удостоверения личности клиента при входе в учетную запись. Такой ключ добавляет "нечто, что у вас есть" к "чему-то, что вы знаете" — информации, которую представляет собой пароль. Двухфакторная проверка подлинности усложняет злоумышленнику взлом учетной записи домена: даже если злоумышленник получает или угадывает имя пользователя и пароль для входа в учетную запись, он также должен иметь ключ. Сегодня существуют многочисленные примеры реализации двухфакторной проверки подлинности, и эта технология распространяется на крупные группы пользователей. SSAC отмечает, что компания VeriSign предложила ввести услугу двухфакторной проверки подлинности "регистратор-владелец регистрации" в рамках процесса оценки услуг регистрации (ПОУР). В этом предложении говорится, что "имя пользователя и пароль, используемые в настоящее время для обработки запросов на обновление, передачу и/или удаление, будут дополнены динамическими кодами доступа" в качестве дополнительной добровольной услуги для регистраторов.³⁰ На этапе 1 предложенного VeriSign процесса будет внедрена двухфакторная проверка подлинности между реестром и регистратором. На втором этапе эта услуга станет доступной для запросов, направляемых от владельца регистрации к регистратору, а также будет включен одноразовый пароль при осуществлении транзакций по протоколу EPP от регистратора к реестру. SSAC предлагает регистраторам рассмотреть это предложение и оценить преимущества, которые они могут получить в случае участия в этой программе. Помимо рассмотрения описанной здесь двухфакторной проверки подлинности, SSAC рекомендует регистраторам обратить внимание на такие методы проверки подлинности и указания, как Руководство по электронной проверке подлинности Национального института стандартов и технологий.³¹

Системы опознавания с помощью вопросов. Отдельные финансовые организации во время настройки учетной записи собирают ответы на целый комплект вопросов, помогающих удостовериться личность. Организация в случайном порядке отбирает несколько из этих вопросов и предлагает ответить на них любому, кто пытается войти в систему. В других организациях пользователю предлагается пара, состоящая из секретного изображения и подписи к нему. Когда пользователь впервые входит в свою учетную запись, он должен выбрать секретное изображение. После этого он составляет подпись к нему. Во время процесса проверки подлинности пользователь должен привести подпись к изображению,

³⁰ VeriSign: услуга двухфакторной проверки подлинности между реестром и регистратором
<http://www.icann.org/en/registries/rsep/>

³¹ http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

прежде чем от него потребуется ввод пароля. Регистраторам предлагается рассмотреть эту меру безопасности в качестве дополнительной услуги для тех клиентов, которые примут неудобство дополнительных вопросов в качестве своеобразной платы за возможность защиты доменных имен и предотвращения неправомерного использования DNS-конфигурации.

Контроль доступа к каждому домену. Доступ к учетной записи регистрации домена предоставляет неограниченный доступ ко всем доменам, зарегистрированным под этой учетной записью, как пользователям, так и злоумышленникам. Аналогом этой часто встречающейся модели управления доступом к регистрационной учетной записи выступает в реальном мире кабинетная модель банковского сейфа: после того как сейф открыт, можно делать все что угодно. Сравните это с банковским хранилищем, содержащим депозитные ячейки: в этом случае пользователь или злоумышленник должен не только открыть вход в хранилище, но еще иметь ключи к каждой депозитной ячейке. Регистраторам предлагается рассмотреть аналогичную модель доступа для клиентов, которые нуждаются в большей степени защиты; например, дополнительная функция предоставит клиенту возможность контролировать, какие каналы связи имеют право вносить изменения в контактную информацию и конфигурацию DNS, инициировать и санкционировать трансфер и т.д.

Множественные, уникальные каналы связи. Организации пользуются преимуществами сохранения точных контактных данных в регистрационных записях доменов. Отдельные организации пользуются также тем, что назначают каждому каналу связи уникальное лицо или должность в организации: в результате возрастает риск того, что о праве на владение заявит кто-либо из организации, а также риск попыток перехвата доменного имени у своего работодателя или клиента работодателя. SSAC рекомендует эти меры регистраторам, которые хотят защитить домены от злоупотреблений со стороны собственного персонала. Эти меры также предоставляют возможность тем регистраторам, которые управляют контактной информацией от имени владельцев регистраций. Например, регистратор может проверить и потребовать уникальные пункты контактной информации, особенно в отношении предпочитаемых средств корреспонденции (электронной почты), в качестве дополнительной функции. Владелец регистрации, так же как и регистратор, может использовать уникальные каналы связи для создания гранулированной модели привилегий. Например, некоторые организации, возможно, захотят убедиться, что только канал связи владельца регистрации может выполнить передачу домена или что только технический специалист может изменить конфигурацию DNS (существуют и другие модели, эти приводятся здесь только в иллюстративных целях). Регистраторы могут предложить владельцам регистраций использовать эти меры в сочетании с другими, например интерактивным подтверждением или уведомлением нескольких получателей.

Изменение уведомлений или подтверждений. В некоторых организациях для защиты от несанкционированных или ошибочных изменений создается специальный рабочий процесс, в рамках которого определенные действия требуют подтверждения нескольких сторон. Множественные подтверждения повышают уровень защиты организации от попыток выдать себя за другое лицо: злоумышленник должен симитировать не одно лицо, а два. Отдельные организации могут быть заинтересованы в использовании услуги, когда регистраторы требуют для проверки несколько каналов связи. Таким образом предприятия могут

распространить те же рабочие процессы, которые они применяют внутри организации, для внесения изменений в контактную информацию, передачи доменов или изменений DNS-конфигурации. Организациям, не имеющим подобных рабочих процессов, регистраторы могут предложить дополнительные услуги по активации таких рабочих процессов от имени клиента. Например, при первоначальной регистрации служба подтверждения изменений регистратора может проверить, предоставил ли заказчик уникальный канал связи для каждого требуемого контактного лица, связанного с доменом. Эта же служба может также позволить заказчику выбрать, какие каналы связи должны быть уведомлены в случае запроса на изменение конфигурации DNS, или потребовать, чтобы как технический, так и административный контакты ответили по телефону или по электронной почте, прежде чем внести какое-либо изменение, запрос на которое поступил от одной стороны. Кроме того, служба подтверждения изменений может помочь предотвратить передачу домена из мстительных или меркантильных соображений. Представьте себе, например, ситуацию, когда сотрудник, выбранный в качестве канала связи, ушел из организации, а организация не изменила контактную информацию с этого сотрудника на его преемника. Если сотрудник ушел недовольным, он может попытаться заявить о своих правах на домен посредством передачи домена. В сценарии со службой подтверждения изменений от других контактов потребуются подтвердить передачу и попытка передачи будет заблокирована.

Уведомления нескольким получателям. Регистраторы обычно пользуются электронной почтой при переписке со своими клиентами. В документе SAC028, Противодействие фишинговым атакам по имитации регистраторов, упоминается несколько обычных видов корреспонденции, включая следующие:

- сообщения о необходимости возобновления доменных имен;
- подтверждения заказа доменных имен;
- подтверждения запросов на регистрацию;
- изменения контактной информации домена и конфигурации DNS;
- напоминания о точности данных «кто есть кто»;
- уведомления об истечении срока действия или аннулировании регистрации доменных имен;
- предложения, рекламные сообщения о (новых) услугах и функциях.

Предложение возможности отправки подобной корреспонденции нескольким получателям может оказать клиентам помощь в нескольких отношениях. Например, клиент может избежать того, чтобы оказаться жертвой фишинговой атаки по имитации: один из получателей клиента может быть введен в заблуждение фишинговым сообщением, но другой может распознать фальшивое сообщение и предупредить регистратора и других контактных лиц в организации. Аналогичным образом, если бы регистратор должен был отправить сообщения о возобновлении доменного нескольким получателям, возникла бы защита от ситуации, когда ошибка или недосмотр клиента могли бы привести к тому, что срок действия регистрации был бы завершен. Например, возобновление может не состояться, если единственный получатель уведомления о возобновлении находится в длительном отпуске и не имеет доступа к электронной почте. В сценарии с несколькими получателями завершения срока регистрации можно избежать, если другие получатели получают уведомление о возобновлении. Регистраторы могут также рассмотреть способы, используемые некоторыми

финансовыми учреждениями для оказания помощи клиентам в обнаружении несанкционированного доступа к учетным записям. Регистратор может попытаться отправить уведомления или подтверждения, используя как исходную, так и измененную версии контактной информации, чтобы повысить вероятность того, что корреспонденция дойдет до нужного адресата независимо от того, предусмотренное это изменение или мошенническое, а также независимо от того, была ли корреспонденция отправлена до или после того, как изменения вступили в силу.

Множественные способы доставки критически важной корреспонденции. Вместо того чтобы полагаться исключительно на электронную почту для переписки с клиентами, регистраторы могут предложить доставлять критически важные уведомления по телефону, факсом, обычной или курьерской почтой тем клиентам, которые хотят получить дополнительные средства защиты. Благодаря таким услугам несанкционированные передачи будут для злоумышленников чрезвычайно затруднены. Заказчики, ожидающие возобновления критически важных доменных имен "навсегда" с удовольствием воспримут эти меры предосторожности (а при обычном порядке вещей эти меры предосторожности не оказывают никакого отрицательного влияния). Заказчики, осуществившие передачу критически важных доменов, могут также посчитать проанализировав риски и преимущества, что задержка, возникшая в ходе "транзакции" передачи, вполне оправданна.

Привлечение заказчика. Многие крупные организации привыкли к аутсорсингу доступа в Интернет, управления безопасностью и сетью. Управляемые услуги также стали популярными среди малых и средних предприятий. Поставщики управляемых услуг развивают партнерские отношения между клиентом и поставщиком. В разделах часто задаваемых вопросов, программе информированности и образования, реализуемой посредством интернет-семинаров и подкастов, поставщики управляемых услуг разъясняют, каким образом клиенты могут извлечь выгоду из предоставляемых ими услуг. В качестве дополнения к мерам, описанным выше, регистраторы могут призвать владельцев регистраций к следующим действиям.

- Определять множественные каналы связи учетных записей доменов.
- Включать управление информацией о каналах связи в процесс управления трудовыми ресурсами, чтобы при аннулировании учетных сведений уволенного работника вся информация о каналах связи для регистрации доменов также была изменена.
- Проводить политику изменения паролей.
- Периодически проверять контакты.
- С упреждением отслеживать регистрацию доменных имен.
- Назначать адреса электронной почты всем регистрационным каналам связи в домене, не совпадающем с зарегистрированным доменом. (Отдельные регистраторы, возможно, захотят создать несколько учетных записей регистрации доменов в качестве дополнительной меры предосторожности).

- Рассматривать попытки передачи как события, имеющие отношение к системе безопасности (проверка и перепроверка).
- Использовать отдельный домен для учетных записей электронной почты регистрационных контактов, не совпадающий с доменами, используемыми для других бизнес-целей. Например, назначить адреса электронной почты каналам связи на example.info, а не на example.net.
- Создавать ролевые учетные записи: например, domainadmincontact@example.com, domainregistrantcontact@example.biz, domaintechnicalcontact@example.net. (Следует иметь в виду, что при использовании ролевых учетных записей настоятельно рекомендуется периодическая проверка таких учетных записей для подтверждения того, что персоналом владельца регистрации ведется непрерывный мониторинг ролевой учетной записи на предмет изменений в составе сотрудников, административных и оперативных изменений в организации).
- Объединять нескольких получателей в ролевую учетную запись для уведомлений. Эта форма почтовой "ковровой бомбардировки" используется при отправке критически важной корреспонденции регистраторов, чтобы повысить вероятность получения корреспонденции и ее своевременной обработки.

Информирование заказчика. Регистраторы должны прилагать все возможные усилия, чтобы настолько же четко информировать заказчика о предпринимаемых мерах безопасности, насколько четкими и убедительными они являются в других конкурентных предложениях. Например, регистратор, который постоянно подвергает свои операции независимой аудиторской проверке мер безопасности и успешно проходит эту проверку, может привлечь внимание общественности к этой возложенной на самого себя обязанности. С другой стороны, ICANN и регистраторы могут совместно выбрать независимого аудитора для проверки системы безопасности и заключить с ним соглашение для определения определенного набора мер безопасности. Регистраторы могут *добровольно* обратиться к аудитору с просьбой о проверке их операций. Регистраторы, успешно прошедшие аудиторскую проверку, могут быть отмечены специальной печатью или штампом, как удовлетворяющие требованиям безопасности. Аналогичные программы используются при выдаче сертификатов SSL соответствующими органами.³²⁻³³ SSAC отмечает, что обработка кредитных карт является обычной процедурой среди регистраторов и что Процедуры аудита мер безопасности в сфере платежных карт для соблюдения торговцами и поставщиками услуг Стандарта безопасности данных могут быть здесь уместными.³⁴

³² Печать сайта Thawte, <https://www.thawte.com/ssl-digital-certificates/trusted-site-seal/index.html?click=site-seal-tile>

³³ VeriSign Secured Seal®, <http://www.verisign.com/ssl/secured-seal/>

³⁴ Совет по стандартам безопасности PCI, <https://www.pcisecuritystandards.org/>

Меры безопасности, отмеченные в предшествующих отчетах SSAC. Многие регистраторы внедрили отдельные или все меры, рекомендованные в разделе 5.2 документа SAC007, Отчет о перехватах доменных имен, *Меры, которые должны предпринять регистраторы для защиты доменных имен*. Эти меры вкратце перечисляются здесь, чтобы представить краткое изложение новых и рекомендованных ранее мер безопасности.

1. Использовать уникальное значение кода EPP authInfo для каждого зарегистрированного доменного имени (а не для каждой учетной записи владельца регистрации доменного имени). Некоторые регистраторы используют одно значение кода EPP authInfo для всех доменов, которыми владеет один владелец. Такая практика подвергает все имена, зарегистрированные клиентом, опасности перехвата на базе одного кода.
2. Установить единое значение по умолчанию для блокировки доменов для всех регистраторов. Многие регистраторы уже блокируют доменные имена автоматически. Регистраторы должны предоставить достаточные инструменты для непосредственной разблокировки доменов, чтобы не произошло неоправданного отказа в запросе на законную передачу от проверенного владельца регистрации доменного имени.
3. Изучать дополнительные способы повышения точности записей владельцев регистрации. Рассматривать возможность использования альтернативных средств связи (например, телефона, в отличие от электронной почты), чтобы владельцы регистраций могли своевременно обновлять сведения и обнаруживать злоупотребления регистрации.
4. Собирать информацию о каналах связи на чрезвычайный случай у владельцев регистраций, регистраторов и реселлеров для сторон, которые могут оказать помощь в срочном восстановлении доменного имени.³⁵ Определять процессы устранения неисправностей (чрезвычайные процедуры), которые согласны исполнять все стороны в тех случаях, когда контакты по чрезвычайным ситуациям недоступны.
5. Рассматривать меры по улучшению проверки подлинности и авторизации, используемых во всех бизнес-процедурах регистраторов.
6. Защищать информацию регистраторов, которая может быть использована для мошенничества и имитации, а также для кражи доменного имени. По умолчанию рассматривать любую информацию, используемую в процессе проверки подлинности регистратора, как конфиденциальную. Рассматривать эту информацию с использованием мер, тождественных или аналогичных используемым для защиты кредитных карт и другой финансовой информации.
7. Улучшать аудит соответствия реселлеров требованиям ведения записей.
8. Обеспечивать понимание реселлерами требований ведения записей регистраторов (и ICANN) и улучшать соответствие этим требованиям.
9. Предоставлять четкую и доступную информацию владельцам регистраций в отношении блокировки доменов и мер по защите доменных имен, предлагаемых регистраторами.

³⁵ См. также документ SAC 038, Контакты регистратора для борьбы со злоупотреблениями, <http://www.icann.org/committees/security/sac038.pdf>

Защита информации о конфигурации DNS от неправомерного использования

Одной из целей получения несанкционированного доступа к учетной записи регистрации домена является приобретение контроля над службой разрешения имен организации. Злоумышленник изменяет имя или IP-адрес серверов объектного имени, чтобы они указывали на систему, которой управляет злоумышленник (обычно ранее зараженный компьютер). На зараженном компьютере злоумышленник размещает DNS-сервер и файл зоны для доменного имени, подвергнувшегося нападению. DNS-сервер злоумышленника разрешает имена домена, подвергнувшегося нападению, и перенаправляет их на вредоносные или имитационные веб-сайты (как было в случае с инцидентами Comcast, ICANN, Panix, и Hush, описанными здесь и в документе SAC007). Отдельные злоумышленники не изменяют злонамеренно информацию о конфигурации DNS; они используют зараженные учетные записи регистрации доменов для добавления своих собственных серверов имен в список законных серверов имен. Это делается, чтобы скрыть используемые ими серверы имен в вариантах *double flux* или атаках Fast Flux³⁶ и затруднить обезвреживание. Оба продлевают время действия фишинга, спама, мошенничества или преступных атак.

Меры, описанные в предыдущем разделе, применимы к тем, кто стремится защититься от несанкционированного использования учетной записи доменного имени заказчика с целью злонамеренного изменения или скрытого добавления информации о конфигурации DNS. В частности, следующие меры, предоставляемые регистратором как дополнительные услуги или осуществленные владельцем регистрации, выполняют функцию мер предосторожности против атак, направленных на конфигурацию DNS.

- Требование многофакторной проверки подлинности для изменений конфигурации DNS.
- Требование подтверждения изменений от нескольких контактов с использованием электронной почты и, возможно, носителей, отличных от электронной почты. (Примечание. Описанные выше способы многоэтапной проверки могут быть использованы и здесь).
- Доставка уведомлений нескольким контактам при внесении изменений.
- Мониторинг изменений DNS на предмет аномалий и злоупотреблений.

Повторим, что регистраторы, посредством разделов с часто задаваемыми вопросами, обучения и просвещения, должны призывать клиентов к непрерывному мониторингу активности конфигурации DNS (изменений и дополнений). Регистраторы также должны призывать клиентов к проверке того, что имена в их домене разрешаются в надлежащие IP-адреса. Кроме того, регистраторы должны призывать клиентов вести журнал конфигураций DNS для всех доменов и помогать им в понимании необходимости применения временной метки и цифровой подписи к этой информации.

³⁶ Документ SAC 025, Хостинг Fast Flux и DNS, <http://www.icann.org/committees/security/sac025.pdf>

Данный документ переведен с английского языка в целях расширения аудитории его читателей. Несмотря на усилия, предпринятые некоммерческой организацией ICANN в отношении проверки точности перевода, единственной официальной версией данного документа, имеющей силу, является англоязычная версия, поскольку английский является рабочим языком ICANN. Исходный документ на английском языке находится по адресу: <http://www.icann.org/committees/security/sac040.pdf>.

Выводы

Из инцидентов и соответствующих исследований, описанных в настоящем отчете, SSAC делает следующие выводы.

Вывод (1) Существуют различия среди регистраторов в отношении их уязвимости для атак и обеспечиваемой степени защиты от атак на учетные записи доменов. У многих регистраторов доменов не имеется достаточной информации, чтобы оценить степень, в которой регистратор способен защитить свои учетные записи доменов от нападений, а конфигурацию DNS от злонамеренного изменения.

Вывод (2) Хотя существует большое количество регистраторов, предлагающих услуги по регистрации доменных имен, ориентированные на потребителя, и меньшее количество регистраторов и организаций по "управлению брэндами", предлагающих услуги безопасности солидным владельцам доменных имен, часто являющимся мишенью атак (как правило, в пакете более широких услуг по защите прав брэнда), SSAC отмечает, что поставщики регистрационных услуг, уделяющие специальное внимание вопросам безопасности, представляют собой редкое явление, отчасти в связи с тем, что оценка мер безопасности не играет решающей роли в решении клиента относительно выбора регистратора, каковую она должна играть.

Вывод (3) Регистраторам следует предоставлять больше информации о доступных их клиентам услугам в области безопасности, чтобы клиенты могли принимать информированные решения. Добровольное предложение своих операций независимым аудиторским проверкам в отношении мер безопасности и публикация успешных результатов подобных проверок позволяет заказчикам выбирать регистратора на основании требований безопасности, а также стоимости и других дополнительных функций (таких, как веб- и DNS-хостинг).

Вывод (4) Регистраторы (и владельцы регистраций) излишне доверяют однофакторной проверке подлинности при входе в учетную запись. Этот способ проверки подлинности был многократно обойден с использованием различных форм социальной инженерии, атак с применением грубой силы и других технологий.

Вывод (5) Мишенью злоумышленников становится конфигурация DNS, когда они достигают успеха в дискредитации учетной записи регистрации домена. В связи с распределенной природой DNS эффект изменения информации о конфигурации DNS сохраняется и после восстановления и соответствующих усилий регистраторов. Вредоносная или неверная DNS-информация может сохраняться по всему Интернету в течение полного времени существования (TTL), связанного с измененной записью DNS-ресурса. Специально в этих целях злоумышленники могут атаковать TTL.

Вывод (6) Обычно после идентификации пользователя в учетной записи или на портале регистрации, пользователь (или мошенник) имеет *глобальные* привилегии и может изменять как контактную информацию, так и информацию о конфигурации DNS. Обеспечение клиентам доступа к управлению гранулированным доступом в качестве дополнительной услуги — в частности, возможность ограничения типа действий, которые может выполнить каждый канал связи в отношении изменения контактной информации и информации о конфигурации DNS, а также авторизации передач — может снизить степень риска неправомерного использования доменных имен и служб разрешения имен, связанных с этими именами.

Вывод (7) Поставщики регистрационных услуг полагаются на неподтвержденные сообщения электронной почты для доставки корреспонденции, связанной с вопросами безопасности (например, уведомлений об изменениях) в большей мере, чем того заслуживают характеристики безопасности и обеспечение доставки электронной почты. Злоумышленники часто обходят этот способ переписки, блокируя доставку электронной почты при изменении конфигурации DNS или доменов с дискредитированных учетных записей регистрации. Предложение клиентам альтернативных возможностей доставки сообщений или включение каких-либо форм уведомления о получении может снизить степень риска неправомерного использования доменных имен и служб разрешения имен, связанных с этими именами.

Рекомендации

Документ SAC007 содержит особые рекомендации для регистраторов, в частности:

Рекомендация SAC007-(8): Регистраторы должны повысить осведомленность владельцев регистраций в отношении угроз перехвата доменных имен, имитации регистраторов и мошенничества и подчеркнуть необходимость соблюдения точности информации регистраторами. Регистраторы должны также информировать владельцев регистраций о доступности и целях статуса Registrar-Lock и поощрять его использование. Регистраторы должны также информировать владельцев регистраций о целях механизмов авторизации (EPP authInfo), развивать рекомендуемую практику защиты владельцами регистраций своих доменов, включая регулярный мониторинг статуса доменного имени, а также своевременное и тщательное обслуживание контактной и авторизационной информации.

На основе анализа последних инцидентов, соответствующего исследования и наших Выводов, SSAC выступает со следующими рекомендациями.

Рекомендация (1) Регистраторам следует предлагать более действенные меры защиты от неправомерного использования услуг регистрации доменных имен для клиентов которые нуждаются в подобных мерах. Меры, перечисленные в данном отчете, могут предлагаться в качестве дополнительных услуг для клиентов, отдельно или в пакете.

Рекомендация (2) Регистраторам следует расширить существующие программы участия в образовательных мероприятиях и разделах часто задаваемых вопросов, чтобы повысить степень осведомленности владельцев регистраций. Регистраторы должны обеспечить более широкий доступ клиентов к информации, касающейся предоставляемых ими услуг в отношении защиты учетных записей регистрации доменов, чтобы клиенты могли принимать информированные решения в отношении мер защиты при выборе регистратора.

Рекомендация (3) Регистраторам следует рассмотреть целесообразность добровольных аудиторских проверок их операций в отношении обеспечения безопасности.

Рекомендация (4) ICANN и регистраторы должны изучить, улучшится ли общее качество регистрационных услуг и получают ли какие-либо преимущества регистраторы в случае назначения независимой утвержденной третьей стороны, которая *по просьбе регистратора* будет проводить аудиторскую проверку безопасности на основании предусмотренного набора мер безопасности. ICANN будет отмечать регистраторов, которые в добровольном порядке успешно пройдут такую аудиторскую проверку, в рамках специальной программы заслуживающих доверия мер безопасности, внедряемой аналогично тому, как органы выдачи сертификатов SSL предоставляют отметки или печати доверия операторам веб-сайтов, удовлетворяющим требованиям безопасности.

Благодарности

Комитет выражает благодарность следующим членам за затраченное время, замечания и рецензии при изучении данного вопроса SSAC:

Яап Аккергиус (Jaap Akkerhuis)
КС Клэффи (KC Claffy)
Стив Крокер (Steve Crocker)
Патрик Фальтстром (Patrik Fältström)
Дункан Харт (Duncan Hart)
Джереми Хичкок (Jeremy Hitchcock)
Родни Джофффе (Rodney Joffe)
Уоррен Кумэри (Warren Kumari)
Дэнни Макферсон (Danny McPherson)
Дейв Пичителло (Dave Piscitello)
Дэн Саймон (Dan Simon)
Джон Шнизлеин (John Schnizlein)
Брюс Тонкин (Bruce Tonkin)
Рик Уэссон (Rick Wesson)
Ричард Вильгельм (Richard Wilhelm)

Заявления о сферах интересов

Биографические сведения о членах SSAC и о сферах их интересов содержатся по адресу:
<http://www.icann.org/en/committees/security/biographies.htm>.

Возражения

Ни один из членов комитета не высказал возражений против публикации этого отчета.