Доклад GNSO о проблемах, связанных с хостингом Fast Flux

СТАТУС ДОКУМЕНТА

Это доклад о проблемах хостинга Fast Flux, запрошенный советом GNSO.

ПРИМЕЧАНИЯ К ПЕРЕВОДАМ

Исходная версия данного документа — это текст на английском языке, доступный по следующему адресу: http://gnso.icann.org/issues/fast-flux-hosting/gnso-issues-report-fast-flux-25mar08.pdf. Если существуют противоречия в переводе или заметные различия между данным документом и исходным текстом, исходная версия имеет приоритетное значение.

КРАТКАЯ ИНФОРМАЦИЯ

Данный доклад предоставлен Совету GNSO в ответ на запрос, полученный от Совета соответственно Прошению, внесенному и принятому на дистанционном совещании Совета 6 марта 2008 г. Доклад был впервые передан Совету GNSO 25 марта. Этот исправленный доклад заменяет предыдущий документ.

СОДЕРЖАНИЕ

1 Сводная информация

Введение

Консультативный совет по вопросам безопасности и стабильности ICANN (SSAC) недавно завершил исследование способа, с помощью которого интернет-злоумышленники могут манипулировать DNS во избежание обнаружения и пресечения своей преступной деятельности. Результаты исследования были опубликованы в январе 2008 года в документе «SSAC Advisory on Fast Flux Hosting and DNS» (Доклад SSAC о хостинге Fast Flux и DNS) (SAC 025)[1], который описывает технологии, называемые общим именем «хостинг fast flux», поясняет возможности, предоставляемые этими технологиями и используемые интернет-злоумышленниками для продления срока существования хостов, применяемых в преступной деятельности, и «призывает ICANN, регистратуры и регистраторов... принять все меры для подавления хостинга fast flux и рассмотреть возможность применения этих мер в дальнейших [аккредитационных] соглашениях».[2]

В ходе дистанционного совещания 6 марта 2008 г.[3] Совет GNSO внес следующее предложение:

> «Рабочая группа ICANN подготовит доклад о проблемах с учетом изменений DNS «fast flux» для рассмотрения Советом GNSO. В частности, рабочая группа рассмотрит доклад SAC [SAC 025] и выделит потенциальные следующие этапы развития политики GNSO, разработанной для подавления возможности использования DNS через IP-адрес «fast flux» или с помощью изменения сервера имен».

В ответ на данный запрос рабочая группа ICANN рассмотрела доклад SAC Advisory (SAC 025) и провел консультации с другими соответствующими и релевантными источниками информации на тему хостинга fast flux.

Определения

Fast Flux

В данном контексте термин «fast flux» относится к быстрому многократному внесению изменений в записи ресурсов A и/или NS в зоне DNS, что приводит к быстрому изменению расположения (IP-адреса), к которому относится доменное имя интернет-хоста (A) или сервера имен (NS).

---

[1] http://www.icann.org/committees/security/sac025.pdf

[2] Несмотря на то, что доклад (SAC 025) относится только к «соглашениям», на презентации SSAC о хостинге Fast Flux, представленной в феврале 2008 г. на конференции ICANN в Дели (http://delhi.icann.org/files/presentation-rasmussen-fast-flux-13feb08.pdf) было четко установлено, что в данном случае подразумеваются «соглашения об аккредитации».

[3] http://gnso.icann.org/meetings/agenda-06mar08.shtml

Single Flux

Разновидность fast flux, при котором быстрое внесение изменений в записи A в файле зоны субдомена (обычно второго или третьего уровня) приводит к быстрому изменению расположения (IP-адреса) интернет-хостов (*например,* веб-сайтов или других серверов содержимого).

Flux сервера имен

Разновидность fast flux, при котором быстрое внесение изменений в записи NS в файле зоны домена высшего уровня приводит к быстрому изменению расположения (IP-адреса) серверов имен одного или нескольких субдоменов.

Double Flux

Разновидность fast flux, при котором для быстрого изменения расположения хостов и серверов имен применяются как single flux, так и flux сервера имен.

Хостинг Fast Flux

Использование приемов fast flux для маскировки расположения веб-сайтов или других интернет-услуг, посредством которых осуществляется противозаконная деятельность.

Сеть Fast Flux

Сеть взломанных компьютерных систем («бот-сеть») с постоянно изменяющимися общедоступными записями DNS.

Рекомендации рабочей группы

Проблемы, связанные с хостингом fast flux, привели к возникновению многочисленных дискуссий между несколькими структурами и заинтересованными сторонами, и могут быть разрешены посредством дальнейшего исследования и анализа. Поэтому рабочая группа рекомендует GNSO финансировать дальнейшие исследования касательно разработки указаний по передовому опыту в отрасли, прежде чем рассматривать целесообразность инициализации формального официального процесса разработки стратегии. К ресурсам рабочей группы будет предоставлен доступ для поддержки этих исследований и целей. Чтобы облегчить процесс принятия решений сообществом, рабочая группа ICANN приветствует предоставление отзывов касательно определенных указаний для дальнейшего исследования.

Несмотря на выбранные организацией GNSO действия, рабочая группа отмечает, что завершение конкретных исследований будет иметь огромное значение для информирования общества в процессе обсуждения.

При определении вхождения вопроса в область процесса стратегии ICANN и организации GNSO рабочая группа и юридический департамент рассмотрели следующие факторы:

- вхождение вопроса в область заявления о миссии ICANN;
- возможность широкого применения вопроса ко многим ситуациям или организациям;
- вероятность наличия у вопроса долговременной ценности или применимости с потребностью в периодических обновлениях;
- возможность создания на базе решения этого вопроса структуры или плана принятия решений в будущем; и
- связь вопроса с существующей стратегией ICANN или влияние на нее.

На основе вышеприведенных данных главный юрисконсульт считает, что некоторые аспекты, относящиеся к хостингу fast flux, находятся в области процесса стратегии ICANN и организации GNSO. Однако главный юрисконсульт также замечает, что вопрос подавления использования хостинга fast flux в интернет-преступлениях шире процесса разработки стратегии GNSO. Некоторые действия, которые можно предпринять для предотвращения или сдерживания хостинга fast flux, например, шаги, которые могут предпринять ccTLD, интернет-провайдеры или сами интернет-пользователи, не находятся в рамках формирования стратегии GNSO. Также затрагиваются домены в ccTLD. Кроме того, рассмотрение вопроса о наличии у возможностей стратегии «долговременной ценности или применимости» имеет особенное значение в контексте хостинга fast flux, когда новые статические правила, введенные процессом разработки стратегии, могут быстро обходить предприимчивые интернет-преступники.

На основе доступной на текущий момент информации рабочая группа рекомендует более тщательно изучать потенциальные возможности развития стратегии. Дальнейшее исследования предоставит требуемые знания для оптимального информирования Совета касательно наиболее эффективных возможностей стратегии. На основе предпочитаемых возможностей впоследствии можно создать основу для запуска определенного процесса разработки стратегии.

2 Цель

Данный отчет предоставляется в ответ на запрос Совета GNSO касательно «Доклада о проблемах хостинга Fast Flux».

В данном контексте, а также в соответствии с подзаконными требованиями ICANN:

a) для рассмотрения предлагается тема хостинга fast flux;
b) лицом, поднимающим вопрос, является Совет GNSO;
c) каким образом данный вопрос затрагивает это лицо: GNSO несет ответственность за разработку стратегии касательно общих доменов верхнего уровня. Хостинг Fast flux часто направлен на домены gTLD (хотя также наблюдается в ccTLD), а организацию GNSO затрагивает проблема фишинга, фарминга и других интернет-преступлений, снижающих стабильную работу и безопасность при использовании Интернета и выполняющихся с помощью приемов, которые могут находиться в рамках ответственности GNSO за разработку стратегии;
d) поддержка вопроса для инициализации процесса PDP: должная поддержка мероприятий, направленных на подготовку данного Доклада о проблемах, была продемонстрирована в ходе дистанционного совещания Совета GNSO 6 марта 2008 г. Разработка Доклада о проблемах была поддержана 10 голосами при 14 голосах «против». Согласно подзаконным актам ICANN вопрос может быть поднят для обсуждения в качестве части процесса PDP, если «его поддержало не менее 25% присутствующих членов Совета…».

3 Введение

Термин «fast flux» относится к быстрому многократному внесению изменений в записи ресурсов A и/или NS в зоне DNS, что приводит к быстрому изменению расположения (IP-адреса), к которому относится доменное имя интернет-хоста (A) или сервера имен (NS). Хотя известны некоторые законные способы использования данного приема (см. ниже), в течение последнего года он стал любимым инструментом злоумышленников и других интернет-преступников, использующих его для избегания обнаружения.

Как работает fast flux[4]

Цель fast-flux – назначение для полностью определенного имени домена (например, *www.example.com*) многих IP-адресов (сотен или даже тысяч). Эти IP-адреса изменяются при входе и выходе из записей A (адрес хоста) и/или NS (сервер имен) файла зоны с чрезвычайной частотой при помощи сочетания цикличных IP-адресов и очень краткого времени существования (TTL). Имена хостов веб-сайтов могут быть связаны с новым набором IP-адресов, которые могут быстро изменяться. Обозреватель, многократно соединяющийся с одним веб-сайтом в течение небольшого периода времени, может в действительности каждый раз соединяться с другим зараженным компьютером. Кроме того, взломщики обеспечивают используемым взломанным системам оптимальную полосу пропускания и доступность услуг. Они часто используют схему распределения нагрузки, учитывающую результаты анализа инфраструктуры узла, для исключения нереагирующих узлов из flux-процесса и обеспечения доступности содержимого.

Переадресация при помощи прокси-серверов добавляет дополнительный уровень запутывания к процессу fast flux. При использовании сети fast-flux пользователем, размещающим зловредное содержание (например, фишинговый сайт), хосты, к которым применялась атака flux (путем быстрого изменения IP-адреса, к которому относится доменное имя), обычно являются прокси-серверами, переадресовывающими запросы на сайт, содержащий действительное содержимое взломщика. Это облегчает действия взломщика, поскольку вместо вынужденного копирования своего зловредного содержимого на большое количество различных ботов он может разместить его на одном хосте и развернуть бот-сеть переадресовывающих прокси-серверов, все из которых указывают на данный хост. Процесс fluxing затем происходит между системами переадресации. Переадресация препятствует попыткам отслеживания и подавления узлов сетей услуг fast-flux. Доменные имена и URL-адреса рекламируемого содержимого больше не относятся к IP-адресу определенного сервера, а вместо этого варьируются между многими входными системами переадресации или прокси-серверами, которые затем в свою очередь переадресовывают содержимое на другую группу выходных серверов. Хотя данный прием какое-то время использовался в сфере законных действий с веб-серверами с целью обеспечения высокой доступности и распределения нагрузки, в этом случае он свидетельствует о технологической эволюции преступных компьютерных сетей.

[4] Основой данного материала (в некоторых случаях, послужившей источником цитирования) является текст описательного характера, расположенный по адресу: http://www.honeynet.org/papers/ff/fast-flux.html.

Базы fast-flux являются управляющим элементом сетей с услугами fast-flux и похожи на системы оперативного управления (C&C), присутствующие в традиционных бот-сетях. Однако по сравнению с типичными серверами бот-сетей базы fast-flux имеют намного больше функций. Именно противоположный основному трафику узел базы fast-flux, скрытый при помощи входных узлов прокси-сетей fast-flux, в действительности возвращает содержимое клиенту-жертве, запрашивающему его. Определенные системы оперативного управления fast flux используют одноранговые (P2P – peer to peer) приложения, поэтому успешно и продолжительно функционируют в естественных условиях. На этих узлах часто наблюдается хостинг услуг DNS и HTTP, при котором настройки виртуального хостинга веб-серверов могут управлять доступностью содержимого одновременно для тысяч доменов на одном хосте.

В сетях fast-flux выполняется много злоумышленных действий, включая онлайновые фармацевтические магазины, сайты незаконного перевода денег «money mule», фишинговые веб-сайты, содержимое для взрослых предельно допустимого или противозаконного характера, веб-сайты для атаки на обозреватели и распространение зловредных загрузок. Кроме DNS и HTTP, при помощи сетей fast-flux можно поставлять другие услуги, например SMTP, POP и IMAP. Поскольку приемы fast-flux используют операции переадресации TCP и UDP, любой направляющий протокол обслуживания с одним целевым портом, вероятно, столкнется с несколькими проблемами при обслуживании через сеть с услугами fast-flux — это не просто веб-сайты; это могут быть также мошеннические почтовые сайты.

Законные способы использования технологии fast flux

Благодаря предварительным исследованиям рабочая группа осознает, что работа некоторых высокомощных систем распределения нагрузки может зависеть от небольших значений времени существования в записях DNS, относящих их главные доменные имена (*например,* www.google.com) к IP-адресам с целью быстрого распространения изменений.[5] Сайт с интенсивным трафиком может использовать данный прием — подпадающий под определение «fast flux» — для адаптации своих адресов домашних страниц к внутренним и внешним условиям сети, например нагрузке на сервер, перебоям в работе, расположению пользователей и перенастройке ресурсов. Поскольку практически все веб-обозреватели помещают проверки доменных имен в кэш-память как минимум на 15-20 минут, независимо от объявленного значения TTL, результирующим эффектом небольшого значения TTL является установка действительного тайм-аута для предупреждения обозревателя. Эти поставщики услуг считают возможность быстрой перенастройки достаточно важной для компенсации дополнительной задержки запросов, вызванной более частыми проверками DNS. Для лучшего понимания сути законных способов использования и их распространения требуется провести дополнительные исследования.

Рабочая группа также осознает, что поставщики услуг могут применить к своим IP-адресам технологию fast-flux в ситуациях, когда правительство или другое лицо умышленно блокирует (создает «черные дыры») свои адреса для предотвращения доступа к их услугам в пределах страны или региона. Этот способ был описан на примерах как возможное «законное использование». Это еще одна сфера, где нужно лучше понять суть обоих технических вопросов для добавления информации в ходе дальнейших исследований.

[5] Информация, полученная рабочей группой, позволила выявить, что значения TTL, эквивалентные промежутку времени в 300 секунд, могут являться стандартными в данных настройках. Тем не менее, для проверки требуется проведение дополнительных исследований.

Почему fast flux является проблемой

Фишинг, фарминг и другие злоумышленные (и часто противозаконные) действия являются широко известной угрозой для защиты и безопасности интернет-пользователей. Лица, занимающиеся этими действиями, могут препятствовать попыткам исследователей, направленных на обнаружение и прекращение их операций с помощью сетей с услугами fast flux для быстрого и постоянного изменения IP-адреса, по которому размещено их содержимое, «оставаясь на шаг впереди» сотрудников правоохранительных органов.

Сети с услугами single-flux изменяют записи DNS для своего IP-адреса входного узла каждые 3-10 минут, поэтому даже при закрытии одного узла системы переадресации flux-агента много других зараженных хостов переадресации находятся в режиме ожидания и доступны для его оперативного замещения. Сети fast-flux в основном создаются из взломанных домашних компьютеров, поскольку в отличие от компьютерной инфраструктуры компании или другой организации с IT-отделом их сложно защитить при помощи мер, направленных против вредоносного ПО.

Сети с услугами fast-flux создают устойчивые и запутанные инфраструктуры поставки услуг, усложняющие закрытие активных мошеннических действий и определение выполняющих их преступников со стороны системных администраторов и судебных органов.

Почему проблема fast flux интересует ICANN

Сообщество исследователей, системных администраторов, сотрудников правоохранных органов и защитников интересов потребителей, борющихся против интернет-мошенничества, возможного благодаря хостингу fast flux или ускоренного при его помощи, пришло к выводу, что попытки препятствования хостингу fast flux путем обнаружения и закрытия бот-сетей (сетей с услугами fast flux) не являются эффективными. Ожидается намного большая эффективность других мер, при которых требуется сотрудничество реестров и регистраторов DNS для определения приемов fast flux и борьбы с ними. ICANN следует рассмотреть целесообразность и способ стимулирования операторов реестров и регистраторов для принятия мер, которые помогут уменьшить убытки, причиненные интернет-преступниками путем понижения эффективности этих атак на основе DNS.

4 Обсуждение возможных направлений

Исследования рабочей группы ICANN подтвердили, что хостинг fast flux:

- является действительным явлением, замеченным, задокументированным и объявленным рядом надежных источников, включая членов Антифишинговой рабочей группы;
- усложняет исследователям определение и прекращение злоумышленной деятельности; и
- его эффективность может быть значительно снижена изменением текущего способа функционирования реестров и регистраторов DNS.

Поскольку хостинг fast flux включает многих разных участников — интернет-преступников и их жертв, интернет-провайдеров, компаний, предоставляющих услуги веб-хостинга, а также реестры и регистраторов DNS — можно представить ряд различных подходов к подавлению. В докладе SSAC определяется три подхода к подавлению, каждый из которых требует сотрудничества различных лиц:

- устранение бот-сетей (пользователи и интернет-провайдеры);
- определение и закрытие хостов fast flux (интернет-провайдеры); и
- изменение способа обработки обновлений зон реестрами и регистраторами, что может уменьшить объем fast flux или сделать его непривлекательным (реестры и регистраторы). Как показано ниже, для дальнейшего изучения эффективности различных возможностей требуются дополнительные исследования и обсуждения.

Эксперты по борьбе с интернет-преступлениями проинформировали рабочую группу, что попытки остановить фишинг и другие виды интернет-мошенничества путем устранения бот-сетей бесполезны. Большинство бот-сетей состоит из взломанных компьютеров, подключенных к домашним сетям с широкополосным доступом (например, при помощи DSL или кабельного соединения), и распространение вредоносного ПО между этими пользователями является чрезвычайно простым; и хотя интернет-провайдеры в некоторых странах могут сотрудничать при определении и устранении бот-сетей, некоторые провайдеры могут быть недоступны и использоваться в качестве «безопасных убежищ» операторами бот-сетей.

Исследователи, противостоящие преступности, и чиновники правоохранных органов часто могут получать распоряжения суда для закрытия фишинг- и фарминг-сайтов при их определении, но fast flux разрабатывается специально во избежание этих попыток «закрытия» путем усложнения отслеживания противозаконной деятельности и определения действительного расположения.

Реестры и регистраторы могут сдерживать эти действия двумя путями: 1) путем отслеживания активности DNS (fast flux легко обнаружить) и предоставления отчетов о подозрительном поведении судебным органам или при помощи другого соответствующего механизма отчетности; 2) путем принятия мер, усложняющих применение или привлекательность fast flux. Предложены некоторые возможные меры, например:

- установка подлинности контактов перед предоставлением разрешения на внесение изменений в записи NS;
- предотвращение автоматического внесения изменений в записи NS;
- применение минимального значения «время существования» (TTL) для ответов на запросы серверов имен[6];
- ограничение количества серверов имен, которые можно определить для данного домена; и
- ограничение количества изменений (A) записей адресов, которые можно внести во время определенного временного интервала в серверы имен, связанные с зарегистрированным доменом[7].

Каждая из предложенных мер может иметь дальнейшие применения, исследование которых рекомендуется рабочей группой. Следует заметить, что процесс разработки стратегии GNSO является одним из нескольких способов, которые можно применить к хостингу fast flux в рамках общества ICANN. В данном разделе описываются разные способы разрешения вопроса для информирования общества ICANN касательно возможных указаний, которыми можно руководствоваться.

---

[6] Промежуток времени в 30 минут был предложен в качестве приемлемого минимального значения TTL. Рабочая группа осознает, что некоторыми регистраторами был внедрен TTL со значением в 30 минут. Реестры и регистраторы могут самостоятельно определять исключительные условия для допустимого использования небольших значений TTL, однако на практике может оказаться достаточно затруднительным провести различие между законным использованием и приложениями преступного характера.

[7] Существует вероятность того, что законной деятельности не будет причинен ущерб в связи с ограничением количества серверов имен до 5 для определенного домена, а также ограничением количества изменений до 5 в месяц.

Разработка указаний по передовому опыту в отрасли

Дополнительные исследования и обсуждения в пределах общества могут привести к разработке набора указаний по передовому опыту в отрасли. В рамках компетенции ICANN они могут сформировать основу для добровольных действий, выполняемых реестрами и регистраторами, или (согласно последующему процессу разработки стратегии) требований, включенных в контракты реестров или соглашения об аккредитации регистратора. Вне непосредственной компетенции ICANN их можно адресовать интернет-провайдерам или другим оператором и поставщикам услуг интернет-инфраструктур в качестве желательных действий и мер, которые они могут добровольно предпринять.

Как утверждается в рекомендациях рабочей группы (см. раздел 5 и «Сводную информацию» в разделе 1), рабочая группа ICANN поддерживает финансирование дополнительных исследований для разработки указаний по передовому опыту в качестве первого этапа, который следует предпринять организации GNSO.

Процесс разработки стратегии GNSO

Рекомендации стратегии по этому вопросу могут выдвинуть новые требования или учредить новые запреты, применимые к связанным договорами сторонам, которые рабочая группа ICANN может впоследствии внедрить и применить благодаря своим контрактам с реестрами и/или регистраторами. Однако ICANN может применить новые требования к реестрам и регистраторам, только если хостинг fast flux является вопросом, «для которого обоснованно необходимо однородное или скоординированное разрешение с целью обеспечения функциональной совместимости, технической надежности и/или устойчивости работы услуг регистраторов, услуг реестров, DNS или Интернета» (раздел RAA 4.2.1).

5 Рекомендации рабочей группы

Как более детально обсуждается ниже, рабочая группа рекомендует GNSO финансировать дополнительные исследования для разработки указаний по передовому опыту касательно хостинга fast flux. Возможно, ccNSO также следует принимать участие в подобной деятельности.

Область применения

При определении вхождения вопроса в область процесса стратегии ICANN и организации GNSO рабочая группа и юридический департамент рассмотрели следующие факторы:

Вхождение вопроса в область заявления о миссии ICANN

Устав ICANN гласит, что:
«Миссией Корпорации Интернета для Специализированных Адресов и Номеров («ICANN») является управление системами уникальной идентификации Интернета на мировом уровне, в том числе, обеспечение стабильности и безопасности работы систем уникальной идентификации Интернета. В частности, ICANN:
1. Управляет назначением и передачей следующих трех типов уникальных интернет-идентификаторов:
    a) доменные имена (которые формируют систему, называемую «DNS» (система доменных имен);
    b) адресов интернет-протокола («IP-адресов») и номеров автономной системы («AS»); и
    c) порт протокола и номера параметров.
2. Координирует работу и развитие серверной системы корневых имен DNS.
3. Управляет политикой развития, имеющей непосредственное отношение к этим техническим функциям».

Хостинг fast flux включает связывание доменных имен с IP-адресами посредством работы серверов имен, включая информацию о переданном домене второго уровня, поддерживающимся регистраторами и реестром для домена TLD, на котором зарегистрирован SLD. Корпорация ICANN несет лишь ограниченную ответственность за разработку стратегии, связанной с этими техническими функциями. В то время, как приведенные выше пункты 1-a) и 3 являются общими темами,

находящимися в рамках заявления о миссии ICANN, некоторые возможности стратегии выйдут за пределы формирования стратегии GNSO.

Возможность широкого применения вопроса ко многим ситуациям или организациям

Рассмотрение вопросов, связанных с хостингом flux hosting, широко применимо к многочисленным ситуациям или организациям, включая каждый существующий gTLD, связанный контрактом с ICANN, каждого из более 800 аккредитованных регистраторов и ряд существующих и потенциальных владельцев регистрации. Однако обратите внимание, что согласованная стратегия, возникшая в результате процесса разработки стратегии GNSO, будет применима только к реестрам и регистраторам gTLD, действующим согласно контракту с ICANN (и только если хостинг fast flux является вопросом, «для которого обоснованно необходимо однородное или скоординированное разрешение с целью обеспечения функциональной совместимости, технической надежности и/или устойчивости работы услуг регистраторов, услуг реестров, DNS или Интернета». Например, см. раздел RAA 4.2.1).

Вероятность наличия у вопроса долговременной ценности или применимости с потребностью в периодических обновлениях

Завершение разработки стратегии касательно вопросов, связанных с темой хостинга fast flux, может повлиять на последующие домены gTLD, регистраторов и потенциальных бизнес- или некоммерческих организаций, еще не вступивших на рынок. Потребуется рассмотреть способы разработки возможностей стратегии, польза от которых будет долговечнее и которые будет тяжелее обойти злоумышленникам.

Возможность создания на базе решения этого вопроса структуры или плана принятия решений в будущем

Результаты процесса разработки стратегии могут иметь долговременную ценность в качестве прецедента, хотя определенные условия рынка продолжат развитие, устанавливая таким образом систему последующего принятия решений касательно связанных вопросов.

Связь вопроса с существующей стратегией ICANN или влияние на нее

Вопрос не связан с существующей стратегией ICANN и не влияет на нее. Список согласованных стратегий доступен по адресу http://www.icann.org/general/consensus-policies.htm.

На основе вышеприведенных данных главный юрисконсульт считает, что некоторые аспекты, относящиеся к хостингу fast flux, находятся в рамках процесса стратегии ICANN и организации GNSO. Поскольку действия хостинга fast flux затрагивают gTLD, вопрос находится в рамках рассмотрения GNSO. Однако вопрос подавления использования хостинга fast flux в интернет-преступлениях шире процесса разработки стратегии GNSO. Некоторые действия, которые можно предпринять для предотвращения или сдерживания хостинга fast flux, например шаги, которые могут предпринять ccTLD, интернет-провайдеры или сами интернет-пользователи, не находятся в рамках формирования стратегии GNSO. Более того, хотя хостинг fast flux часто направлен на домены gTLD, он также наблюдается в ccTLD. Кроме того, рассмотрение вопроса наличия у возможностей стратегии «долговременной ценности или применимости» имеет особенное значение в контексте хостинга fast flux, когда интернет-преступники могут быстро обходить статические стратегии. На основе доступной на текущий момент информации рабочая группа рекомендует более тщательно изучать потенциальные возможности развития стратегии. Дальнейшее исследования предоставит требуемые сведения для оптимального информирования Совета касательно доступных возможностей стратегии с наибольшей эффективностью. На основе предпочитаемых возможностей впоследствии можно создать основу для запуска определенного процесса разработки стратегии.

Рекомендуемые действия

Рабочая группа рекомендует GNSO финансировать дополнительные исследования для разработки указаний по передовому опыту касательно хостинга fast flux и предоставлять данные для содействия разработке стратегии и освещения потенциальных возможностей стратегии. Разработка передовых практических методов должна выполняться путем широкого сотрудничества с информированными лицами и организациями, и к ней также должен предоставляться широкий доступ для стимулирования значительного вклада в ее рассмотрение и широкого принятия. Некоторые регистраторы могут уже внедрять часть мер, определенных в документе SAC 025, и рабочая группа рекомендует консультироваться у этих регистраторов для определения эффективности данных мер и оптимальных способов их внедрения. К ресурсам рабочей группы можно предоставить доступ для поддержки этих исследований и целей.

Изучение советом SSAC хостинга fast flux, а также несколько отраслевых статей сфокусированы на следующих важных вопросах, включая:

- Кому fast flux приносит пользу, а кому – вред?
- Кому принесет пользу прекращение этих действий, а кому – вред?
- Каким образом в деятельность, связанную с хостингом fast flux, вовлечены операторы реестра?
- Каким образом в деятельность, связанную с хостингом fast flux, вовлечены регистраторы?
- Как хостинг fast flux влияет на владельцев регистрации?

Ниже перечислены некоторые дополнительные вопросы, которые можно сделать объектом исследования:

- Как хостинг fast flux влияет на интернет-пользователей?
- Какие принудительные нормы можно применить для уменьшения или устранения отрицательных эффектов хостинга fast flux?
- Как повлияет (положительно или отрицательно) установление ограничений или указаний для регистраторов и/или реестров относительно приемов, которые делают возможным хостинг fast flux или обеспечивают его выполнение?
- Какие меры следует внедрять реестрам и регистраторам для подавления отрицательных последствий fast flux? Следует ли документировать эти меры и распространять их в качестве «отраслевых передовых практических методов», включенных в контракты реестров и соглашения об аккредитации регистратора, либо пропагандировать каким-либо иным образом?

Приложение 1 – Запрос GNSO доклада по проблемам, связанным с хостингом Fast Flux

В данном приложении полностью воспроизведен запрос доклада по проблемам, отправленный Советом GNSO:

Поскольку технология DNS fast flux все чаще используется для совершения преступлений и препятствования деятельности по борьбе с нарушениями посредством динамического изменения IP-адресов и/или серверов имен, чтобы избежать обнаружения и закрытия вредоносных веб-сайтов;

Поскольку Консультативный комитет по вопросам безопасности и стабильности (SSAC) сообщил о данной тенденции в своем докладе Advisory SAC 025 за январь 2008 г.: http://www.icann.org/committees/security/sac025.pdf/

Поскольку в докладе SSAC Advisory описываются технические аспекты хостинга fast flux, объясняется использование DNS для содействия правонарушениям, обсуждаются текущие и возможные методы борьбы с такими нарушениями, а также содержатся рекомендации для всех соответствующих организаций по рассмотрению стратегий, которые могут сделать практические методы борьбы доступными в равной мере для всех владельцев регистрации, интернет-провайдеров, регистраторов и реестров,

Поскольку GNSO, вероятно, является соответствующей стороной, которая должна рассматривать такие стратегии

Совет GNSO ПРИНИМАЕТ РЕШЕНИЕ

Рабочая группа ICANN подготовит доклад о проблемах, касающихся изменений DNS «fast flux», для рассмотрения Советом GNSO. В частности, рабочая группа рассмотрит доклад SAC [SAC 025] и выделит потенциальные следующие этапы развития политики GNSO, разработанной для подавления возможности использования DNS через IP-адрес «fast flux» или с помощью изменения сервера имен.