Дата: 26 января 2009 г.

RU

Сводное резюме

Предварительный отчёт
Рабочая группа GNSO по хостингу Fast Flux

СТАТУС ДОКУМЕНТА

Данный документ представляет собой сводное резюме предварительного отчёта рабочей группы по хостингу fast flux.

Примечание к переводам

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. Обратите внимание: данное сводное резюме представляет собой только одну главу из полной версии доклада, доступной исключительно на английском языке. Полная версия опубликована на веб-сайте по адресу http://gnso.icann.org/.

Дата: 26 января 2009 г.

RU

СОДЕРЖАНИЕ

1 СВОДНОЕ РЕЗЮМЕ 3

1 Сводное резюме

1.1. История

- В соответствии с публикацией информационного бюллетеня SSAC по хостингу Fast Flux и DNS (SAC 025) в январе 2008, Совет GNSO 6 марта 2008 года дал поручение персоналу ICANN подготовить и выпустить отчет , в котором рассматривается Рекомендация SAC [SAC 025], и очерчиваются следующие потенциально возможные шаги по разработки политики GNSO, направленной на смягчение имеющихся в настоящее время возможностей для криминальных элементов использовать DNS через IP fast flux' IP или изменение имени сервера'.
- Отчёт по этим проблемам был опубликован 31 марта 2008 года. Было рекомендовано "спонсору GNSO искать дальнейшие факты и исследовать относящиеся к этому директивы по передовой практике отрасли перед тем, как рассмотреть вопрос о том, следует ли инициировать формальный процесс разработки политики".
- На собрании 8 мая 2008 г. Совет GNSO официально запустил процесс разработки политики (PDP) и призвал к созданию рабочей группы по Fast flux. Устав рабочей группы был утвержден 29 мая 2008 года, рабочей группе было предложено рассмотреть следующие вопросы:
  - Кто выигрывает от Fast flux, а кому наносится ущерб?
  - Кто выиграет от прекращения использования этого метода, а кто пострадает?
  - Связаны ли или могут ли быть связаны операторы реестра с действиями, касающимися Fast flux? Если да, то как?
  - Связаны ли регистраторы с действиями, касающимися Fast flux? Если да, то как?
  - Как Fast flux влияет на регистрирующихся лиц?
  - Как Fast flux влияет на пользователей Интернета?
  - Какие технические (например, изменения в способе функционирования обновлений DNS) и политические (например, изменения в соглашениях реестр/регистратор или правилах, устанавливающих допустимое поведение регистратора) меры могут выполняться реестрами и регистраторами для смягчения отрицательного влияния Fast flux?

- Каким будет эффект (положительный или отрицательный) от введения лимитов, директив или ограничений, касающихся зарегистрированных лиц, регистраторов и/или реестров с учетом методик, позволяющих или способствующих Fast flux?
- Каков будет эффект этих лимитов, директив или ограничений на инновации в услугах и продуктах?
- Каковы наилучшие доступные методики с учетом защиты от Fast flux?

Группе также была поставлена задача получить мнения экспертов, там, где это уместно, по тем областям применения Fast flux, которые выходят за пределы сферы разработки политики GNSO.

1.2. Подход, используемый рабочей группой

- Рабочая группа по Fast Flux начала обсуждение работы 26 июня 2008 года и приняла решение начать работу с вопросов поставленных в уставе при параллельной подготовке заявлений для аудитории по этой теме. Чтобы облегчить обратную связь от заинтересованных сторон, были разработаны шаблоны для ответов (см. приложение I). В дополнение к еженедельным конференциям возник интенсивный диалог в виде почтовой рассылки по теме "fast flux" с более чем 800 сообщениями.
- Если не указано иное, положения, очерченные в этом документе подлежат согласованию Рабочей группой. Там, где соглашение в общих чертах не может быть достигнуто, должны использоваться указанные ниже пометки для указания уровня поддержки определенной позиции:
  - Поддержка – имеется определенное положительное мнение, однако могут существовать противоположные позиции и соглашение в целом не было достигнуто.
  - Альтернативная точка зрения – мнение отличающееся от выраженного, и не имеющее достаточной поддержки в Рабочей группе, чтобы заслужить статуса "поддержка" или "согласие". Следует обратить внимание, что альтернативная точка зрения может быть выражена и при наличии соглашения в целом и поддержки.

1.3. Обсуждение вопросов устава

- Для целей рабочей группы агрессивная сеть fast flux имеет следующие характеристики:
  - некоторые, но не обязательно все узлы сети работают на подверженных риску хостах (например, используется программное обеспечение, которое было установлено на хостах без уведомления или разрешения оператора/владельца системы);
  - изменчивость в том смысле, что активные узлы сети изменены для того, чтобы обеспечить срок службы сети, облегчить распространение сетевых компонентов программного обеспечения и проводить другие атаки; и
  - используются различные методы для достижения изменчивости:
    - быстрый и повторяющийся выбор систем из пула хостов, с которыми эти системы используются в целях обслуживания вредоносного контента, для использования в качестве серверов имен или в других целях, причем все вышеуказанное осуществляется через входы DNS с низкими значениями времени существования (TTL);
    - распределение узлов сети по большому числу автономным систем потребительского класса;
    - мониторинг узлов членов сообщества с целью определения/вывода о том, что хост идентифицирован и отключён; и
    - время или другие основанные на метрической базе изменения топологии в узлах сети, сервере имени, прокси-объектах или других компонентах.

    Дополнительные характеристики, которые в сочетании или в совокупности используются для распознавания или "снятия отпечатков" атак fast flux, включают следующее:
    - несколько IP-адресов на NS, образованных несколькими ASN,
    - частые изменения NS,
    - in-addrs.arpa или IP-адреса, находящиеся в блоках размещения шировещательного потребительского диапазона,
    - возраст доменного имени,
    - низкое качество службы "Кто есть кто",

- определение того, что прокси-сервер nginx работает на рассматриваемой машине: nginx обычно используется для нелегальных скрытых/прокси веб-серверов,
- доменное имя является одним из возможных доменных имен зарегистрированного лица, чья учетная запись администратора домена была скомпрометирована, а атакующая сторона изменила информацию о доменном имени без разрешения.

- Распределение и использование программного обеспечения, установленного на хостах без уведомления или согласия оператора/владельца системы, является критически важной характеристикой атаки сети fast flux; в частности, это является одной из нескольких характеристики, которые отличают агрессивные сети fast flux от работы с использованием технологии fast flux в приложениях, таких как сет распределения контента, высокодоступная и мобильная сеть, и т.д.
- При использовании криминальными элементами основной целью хостинга fast flux является продолжительный период времени, в течение которого атака продолжает быть эффективной. Это не атака как таковая – это способ атакующего избежать обнаружения и свести на нет реакцию на атаку.
- Рабочая группа предложила следующие первые ответы на вопросы, заданные в уставе, однако хотела бы подчеркнуть, что необходимо продолжение работы в следующих областях:
  - Надёжное техническое и процессуальное определение “fast flux”,
  - Надёжные методы для определения сетей fast flux, в которых поддерживается приемлемая частота ложных срабатываний,
  - Надёжная информация в отношении объёма и проникновения сетей fast flux,
  - Надёжная информация в отношении финансового и нефинансового влияния сетей fast flux,
- Вопросы устава:

1. <u>Кто выигрывает от Fast flux, а кому наносится ущерб?</u>

Кто выигрывает от Fast flux?

- Организации, которые управляют сетями с высокоопределяемыми целями
- Сети распределения контента
- Группы свободы слова / агитационно-пропагандистские организации

Кто страдает от действий fast flux?

- Рабочая группа обращает внимание, что возможно как законное, так и причиняющее ущерб использование технологий Fast flux. Члены рабочей группы обнаружили эту трудность во время своего обсуждения с тем, чтобы провести чёткое различие между ущербом, который возникает от применения самого метода, и ущербом, который возникает от незаконных действий “правонарушителей”, которые могут использовать fast flux в качестве одного из методов, позволяющих избежать их обнаружение.
- Рабочая группа не достигла согласия по поводу раздельной идентифицируемой виновности хостинга fast flux в отношении ущерба, вызванного незаконными действиями, но признала, что выявила способ, которым технологии fast flux используются для продления атаки.

2. Кто выиграет от прекращения использования этого метода, а кто пострадает?

Стороны, которые выиграют от прекращения использования этого метода те же, которым причиняется ущерб при использовании fast flux для поддержки агрессивных fast flux. Поэтому рабочая группа сосредоточила свое внимание на идентификации сторон, которым причиняется ущерб.

- Лица, чьи компьютеры заражены атакующими и впоследствии используются для хостинга технического обеспечения агрессивных сетей fast flux.
- Предприятия и организации, чьи компьютеры заражены атакующими, и впоследствии используются для хостинга технического обеспечения агрессивных сетей fast flux.
- Лица, которые получили фишинговое электронное сообщение и зашли на фишинговый сайт, который выполняет fast flux атаку на сеть, могут обнаружить недостачу денег на кредитной карте, пострадать от нарушения безопасности или банковского мошенничества.
- Провайдеры Интернет-услуг могут пострадать в случаях, когда их IP-адреса блокируются, а доменные имена связываются с агрессивными сетями fast flux. Провайдеры Интернет-услуг могут также понести убытки из-за отвлечения персонала и ресурсов на контроль и устранение неполадок.

- Репутация регистратора может пострадать, если он регистрирует, а службы хостинга DNS используются для организации агрессивных сетей fast flux с применением технологии “double flux”. Регистратор может также понести убытки из-за отвлечения персонала и ресурсов на контроль и устранение неполадок.
- Предприятия и организации, которые получают фишинговые сообщения с поддельных веб-сайтов, расположенных в агрессивных сетях fast flux.
- Лица или предприятия, на жизнь или средства к существованию которых влияют незаконные действия, осуществляемые посредством агрессивных сетей fast flux.
- Реестр может понести убытки из-за отвлечения персонала и ресурсов на контроль и устранение злоупотреблений.

Кто получает выгоду от использования технологий Fast flux?

- Организации, которые управляют сетями с высокоопределяемыми целями
- Сети распределения контента
- Организации, которые предоставляют каналы для свободы слова, малочисленных агитационно-пропагандистских или революционных организаций
- Криминальные элементы, террористы и, в целом, любая организация, которая использует агрессивные сети fast flux

Рабочая группа признает, что использование этой технологии в будущем может быть развито, и в результате можно будет пополнить список выгод от её применения.

3. Связаны ли или могут ли быть связаны операторы реестра с действиями, касающимися Fast flux? Если да, то как?

В своем официальном отчете комитет реестров представил подробные комментарии относительно метода и возможностей ведения политики, доступных операторам реестра в отношении хостинга fast flux (см. приложение III).

4. Связаны ли регистраторы с действиями, касающимися Fast flux? Если да, то как?

- Большинство регистраторов не вовлечены в fast flux или double-flux
- В тех случаях когда домены fast flux зарегистрированы мошенниками, подавляющее большинство регистраторов являются невольными участниками этих схем
- Некоторые регистраторы, а еще чаще реселлеры услуг регистраторов по-видимому, способствуют атакам домена fast flux.
- Ни один регистратор не преследовался законом за помощь в криминальной деятельности, связанной с доменами fast flux, однако имеются отчёты, связывающие одного ICANN-аккредитованного регистратора с большим количеством мошеннических доменов, включая домены fast flux.

Кроме того, в отчёте описан ряд известных направлений атак, а также контрмеры.

5. Как Fast flux влияет на зарегистрированных лиц?

Зарегистрированные лица являются мишенями лиц, использующих атаки fast flux, которые ищут доменные имена, которые можно использовать для облегчения атак double flux. Атакующих привлекают существующие домены, которые имеют положительную репутацию по сравнению с вновь зарегистрированными доменами в силу их возраста и истории. Эти факторы являются важными для исследователей, которые пытаются определить, является ли домен связанным с атаками fast flux.

6. Как Fast flux влияет на пользователей Интернета?

Пользователи Интернета предоставляют материалы, на которых работает fast flux (зараженные вирусами потребительские компьютеры, использующие широкополосную передачу), и в тоже время служат мишенями для содержащих спам веб-сайтов, используемых для атак fast flux.

7. Какие технические (например, изменения в способе функционирования обновлений DNS) и политические (например, изменения в соглашениях реестр/регистратор или правилах, устанавливающих допустимое

поведение регистратора) меры могут выполняться реестрами и регистраторами для смягчения отрицательного влияния Fast flux?

Рабочая группа хочет подчеркнуть, что технология fast flux нуждается в лучшем определении и исследовании. Идеи, представленные здесь, являются планом для постепенного развития. Решения подразделяются на две категории на основании типа вовлечения, ожидаемого ICANN и его контрактными или аккредитованными сторонами (регистры и регистраторы gTLD): те которые потребовали бы всего лишь доступности дополнительной или более точной информации, которая может быть использована (или не использована) другими сторонами, вовлеченными в антимошенническую деятельности и сопутствующие мероприятия, которые они сочтут уместными (сбор информации); и те, которые потребовали бы или как минимум будут выгодными до некоторой степени в результате участия ICANN и/или регистров и регистраторов для идентификации и сдерживания мошеннических или других “вредоносных” действий (активные действия).

- Сбор информации – обмен информацией, предложенной к обсуждению, которая включает следующие идеи:
    - Получение дополнительной неперсонализированной информации о зарегистрированных доменах, доступных по через DNS на основе запросов;
    - Опубликованные сводки по уникальным томам жалоб по регистратору, TLD и серверу имени;
    - Поощрение поставщиков услуг Интернета оснащать инструментами свои собственные сети;
    - Объединение инициатив, предназначенных для облегчения разделения данных и идентификации проблемных доменных имен.
- Активное сотрудничество – обсуждаемые идеи по активному сотрудничеству включают:
    - Использовать ускоренную обработку приостановленных доменов в сотрудничестве с сертифицированными исследователями / исполнителями;
    - Определить руководства по использованию специфических методов, таких как очень низкие значения TTL;

- Идентифицировать серверы имен как статичные или динамичные при регистрации домена регистратором;
- Брать номинальную стоимость за изменение статичного IP-адреса сервера имени;
- Позволять Интернет-сообществу подавлять хостинг fast-flux теми же способами, какие применяются в случае других нарушений правил использования;
- Жёстче использовать процедуры верификации регистратора.

8. Каким будет эффект (положительный или отрицательный) от введения лимитов, директив или ограничений, касающихся зарегистрированных лиц, регистраторов и/или реестров с учетом методик, позволяющих или способствующих Fast flux?

Любая попытка Рабочей группы ответить на этот вопрос откладывается до тех пор, пока следующие официальные заявления и комментарии общественности, в частности, запрошенные по этому вопросу, не будут получены и рассмотрены Рабочей группой.

9. Каков будет эффект этих лимитов, директив или ограничений на инновации в услугах и продуктах?

Любая попытка Рабочей группы ответить на этот вопрос откладывается до тех пор, пока следующие официальные заявления и комментарии общественности, в частности, запрошенные по этому вопросу, не будут получены и рассмотрены Рабочей группой.

10. Каковы наилучшие доступные методики, направленные на защиту от Fast flux?

В мире фишинга можно найти один источник по передовой практике защиты от fast flux. Антифишинговая рабочая группа недавно выпустила документ по передовой практике для регистраторов доменов касающийся доменных имен, зарегистрированных фишерами (“Anti-Phishing Best Practices Recommendations for Registrars” http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf). Некоторые

из методов, определенные в этом документе, прямо или косвенно применимы к доменным именам fast flux.

Кроме того, в документе SAC 035 определены методы миграции, используемые сегодня на практике определенными регистраторами в случае, когда регистратор предоставляет DNS для клиентских доменов.

11. **Получить мнения экспертов, там, где это уместно, по областям применения Fast flux, выходящим за пределы сферы разработки политик GNSO.**

Некоторые члены Рабочей группы излагают причины относительно того, почему разработка политики борьбы с fast flux находится за пределами сферы компетенции ICANN, тогда как другие с этим не согласны. Поиск сведений рабочей группой и работа над определениями документально подтвердили, что fast-flux связан, скорее, с проблемами использования доменного имени, а не с проблемами регистрации доменного имени.

1.4. Проблемы

Несмотря на тот факт, что рабочая группа выполняла свою работу с большим энтузиазмом и самоотверженностью, возник ряд проблем, которые указаны в шестой главе, таких как отсутствие согласованности по поводу определения fast flux и поддержке данных, а также неправильное понимание масштабов процесса разработки политики и сферы компетенции ICANN.

1.5. Промежуточные выводы

- Получение общей оценки и широкое понимание мотивации, лежащей в основе использования технологий fast flux или адаптивного создания сети, представляло особенно острую проблему для Рабочей группы. Попытки выявить другие назначения, кроме криминальных, и охарактеризовать хостинга fast flux как законный или незаконный, хороший или плохой, вызвали большие разногласия.
- Исследование, выполненное членами Рабочей группы, выявило, что хостинг fast flux однозначно и точно характеризуется как “быстро изменяющийся”, но в более общем смысле хостинг fast flux включает в себя ряд вариаций и адаптаций, чувствительных к событиям, легко реагирующих или изменчивых технологий.

- Рабочая группа признает, что fast flux и похожие технологии являются всего лишь компонентами большой проблемы мошенничества и правонарушений в Интернете. Методы, описанные в этом отчёте, являются лишь частью огромного и постоянно развивающегося набора инструментов атакующих: подавление одного из этих методов не устранит проблему мошенничества и правонарушений в Интернете.
- Эти различные и сильно взаимосвязанные между собой проблемы должны приниматься во внимание при всех потенциальных процесса разработки политики и/или следующих этапов. К вопросу относительно роли ICANN в этом процесс необходим осторожный подход.

1.6. Возможные следующие шаги

Примечание: рабочая группа хотела бы представить новые идеи для обсуждения и обратной связи в период публичного рассмотрения проблемы. Пожалуйста, обратите внимание, что на этом этапе Рабочая группа не достигла согласия по каждой из указанных ниже идей. Целью рабочей группы будет рассмотрение мнений, полученных во время периода публичного обсуждения и определение того, какие рекомендации (если таковые будут) получат поддержку Рабочей группы для включения в окончательный отчет.

- Переопределить проблему и объем задач путем разработки нового устава или выполнения дальнейшего исследования и поиска сведений до того, как будет разработан новый устав.
- Использовать возможность вовлечения других заинтересованных сторон в процесс разработки политики в отношении fast flux.
- Использовать другие средства для решения проблемы, отличные от процесса разработки политики.
- Выявить, какие решения/рекомендации можно выполнить с использованием разработки политики, передовой практики и/или промышленных решений.
- Рассмотреть, помогут ли меры политики в отношении нарушений регистрации справиться с fast flux силами уполномоченных регистров/регистраторов путём аннулирования доменного имени, вовлеченного в fast flux.
- Использовать возможность разработать систему сообщения о данных Fast Flux (FFDRS).