SAC 025
Рекомендации SSAC относительно хостинга Fast Flux и DNS

ПРИМЕЧАНИЯ К ПЕРЕВОДАМ

Исходная версия данного документа на английском языке доступна по следующему адресу: http://www.icann.org/committees/security/sac025.pdf. При наличии противоречий в переводе или различий между данным документом и исходным текстом исходная версия имеет приоритетное значение.

Рекомендации Консультативного комитета по вопросам безопасности и стабильности (SSAC) ICANN
Январь 2008 г.

Предисловие

Fast flux – это метод маскировки, позволяющий интернет-злоумышленникам скрыть информацию о себе и препятствовать деятельности правоохранительных органов, направленной на поиск и закрытие веб-сайтов, используемых в незаконных целях. Хостинг Fast flux позволяет совершать большое количество интернет-преступлений (мошенничество, кражу личных данных, разные виды сетевого мошенничества) и на сегодня считается одной из наиболее серьезных угроз в Интернете. Один из вариантов хостинга fast flux является double flux, использующий регистрацию имен доменов и сервисы разрешения имен.

В данном докладе Advisory описываются технические аспекты хостинга и сетей fast flux. В нем объясняется, как с помощью DNS можно способствовать совершению преступлений с использованием хостинга fast flux, а также определяется влияние хостинга fast flux и уделяется особое внимание тому, как подобные атаки продлевают срок вредоносного или прибыльного использования противозаконных действий, осуществляемых при помощи данных методов fast flux. В нем описываются текущие и возможные методы предотвращения хостинга fast flux в различных расположениях в Интернете. В докладе Advisory приводятся преимущества и недостатки этих методов предотвращения, определяются методы, которые SSAC считает практичными и целесообразными, а также содержатся рекомендации для всех соответствующих организаций по рассмотрению стратегий, которые могут сделать практические методы предотвращения доступными в равной мере для всех владельцев регистрации, провайдеров услуг Интернета, регистраторов и реестров (в применимых случаях для каждого из них).

Введение

Специалисты по безопасности, сообщество по борьбе с интернет-преступлениями и судебные органы некоторое время изучали хостинг fast flux как явление. Хостинг fast flux использует большую, распределенную сеть взломанных систем, которая может легко распространяться во всем мире. Процветающий подпольный бизнес работает по принципу сдачи в аренду злоумышленникам от десятков до тысяч взломанных систем как сетей fast flux[1]. Операторы таких сетей используют иерархические скрытые (зашифрованные) каналы связи и приемы прокси-серверов. Они старательно управляют этими сетями, периодически запрашивая состояние взломанных сетей, а база добавляет и удаляет компьютеры из сетей на основе наличия или отсутствия ответа. Особый интерес для сообщества доменных имен представляет способ, посредством которого эти операторы автоматизируют обновления служб доменных имен для сокрытия расположения веб-сайтов, с помощью которых осуществляются противозаконные действия – IP-пиратство (музыка, видеозаписи, игры), размещение детской порнографии и фишинговых систем, противозаконная продажа фармацевтических средств, кража личных данных и мошенничество.

[1]Организации, отвечающие за безопасность, используют различный набор терминов при описании хостинга fast flux в литературе и публикациях. В данном документе Advisory нами используется терминология из «Honeynets Project Report, *Know Your Enemy: Fast Flux Service Networks» (Отчет проекта сетей Honeynet: знать своего врага. Сети с предоставлением услуг Fast Flux)*, см. http://www.honeynet.org/papers/ff/

В одном из вариантов хостинга fast flux используются оперативные обновления DNS-информации для маскировки расположения веб-сайтов и других интернет-услуг, посредством которых осуществляется противозаконная деятельность. Второй вариант, называющийся «double flux», состоит в дополнении интернет-преступниками сети, в которой размещены веб-сайты, другой сетью с DNS-серверами. Функционирование данных сетей услуг подробно описывается в следующих разделах данного доклада Advisory.

Терминология

Для наиболее полного описания этого сложного и многогранного метода fast flux SSAC сначала определяет несколько терминов, которые сообщество интернет-безопасности связывает с хостингом fast flux:

Бот-сеть. Бот-сеть – это сеть взломанных компьютеров сторонних лиц, на которых запущены программные роботы (или боты). Этими ботами можно управлять на расстоянии (сначала это делает взломщик, а впоследствии – лицо, которое арендует бот-сети), контролируя неограниченное количество несанкционированных или противозаконных действий. Взломщик обычно связан с организованными криминальными структурами. Взломщик устанавливает на компьютере «программу-бот» без уведомления или авторизации путем загрузки шпионского ПО или вируса, вложенного в сообщение электронной почты, а чаще – через обозреватель или другие средства на стороне клиента (например скомпрометированный рекламный баннер). Когда бот готов к запуску, он устанавливает обратный канал связи с управляющей инфраструктурой, настроенной взломщиком. В традиционной структуре бот-сети использовалась централизованная модель, при которой все обратные каналы связи соединялись с центром оперативного управления взломщика (C&C). В последнее время операторы бот-сетей используют для обратных каналов связи одноранговые модели, чтобы воспрепятствовать обнаружению центра C&C с помощью анализа трафика.

Бот-мастер. Архитектор-злоумышленник распределенной атаки, используемой для создания, поддержки и использования бот-сети в финансовых или иных (политических) целях. После установки бот-сети бот-мастер сдает ее в аренду, чтобы помочь **оператору услуг Fast Flux**

Fast flux. Используется для обозначения способности быстрого перемещения расположения веб-сайта, почтового сервера, DNS или любой Интернет-службы или распределенной службы с одного или нескольких компьютеров, подключенных к Интернету, к другому набору компьютеров, чтобы замедлить процесс обнаружения или избежать его.

Средства Fast Flux. В данном документе термин *средство* обозначает программного агента, установленного без согласия на большом количестве компьютеров с подключением к Интернету.

Сеть Fast Flux. В данном документе сетью услуг называется подгруппа ботов, назначенных бот-мастером определенному оператору услуг Fast Flux, который в свою очередь предоставляет своему клиенту средства для хостинга fast flux или службы имен. Следует отметить, что данной сетью услуг часто управляет «посредник», а не сам клиент.

Структура хостинга Fast Flux

Ниже описан пример хостинга fast flux. Другие проявления и варианты похожи на описанный образец хостинга, причем взломщики могут в дальнейшем изменить методы хостинга fast flux во избежание обнаружения с помощью способов, описанных в данном документе, либо добавить дополнительные уровни иерархии или абстракции.

Много внимания уделяется техническим аспектам fast flux, но существует также связанный набор «бизнес-операций», который необходимо описать. Ниже рассматривается случай, когда преступник планирует провести фишинговую атаку.

Первое звено в организации хостинга fast flux – авторы вредоносного ПО. Некоторые авторы вредоносного ПО разрабатывают наборы для фишинга – комплекты программ, которые можно настроить для отправки фишингового сообщения электронной почты группе получателей и размещения связанного противозаконного веб-сайта в расположении, ссылка на которое находится в сообщении. Другие авторы собирают адреса электронной почты и продают эти списки для отправки нежелательной почты. Некоторые авторы разрабатывают программные боты. Программный бот – гибкий агент, управляемый на расстоянии, который может выполнять произвольные функции от имени соответствующей программы **центра оперативного управления** (C&C): после тайной установки в небезопасной системе программный бот облегчает процесс последующих загрузок и удаленное выполнение дополнительных программ, предназначенных для атаки. Бот-мастера часто используют вложенные в сообщения электронной почты черви для заражения и взлома тысяч систем, хотя на сегодня наиболее распространенными являются клиентские взломы, например атаки с использованием обозревателей.

Авторы вредоносного ПО и бот-мастера являются *поставщиками товаров* в сообществе интернет-преступников. Поставщики товаров используют зашифрованные и частные/защищенные каналы интернет-чатов (iRC) или подобные закрытые места встреч для рекламирования своих противозаконных товаров и поиска покупателей[2]. Противозаконные товары бот-мастера – это средствами, которые он может предоставлять бесплатно или сдавать в аренду. Мастер сдает клиенту в аренду средства управления определенным количеством взломанных систем, которые клиент может использовать непосредственно или через другого посредника; в последнем случае клиент бот-мастера является поставщиком услуг хостинга fast flux. В этой сложной и тайной системе сторона, заинтересованная в совершении правонарушений, может вести переговоры с несколькими сторонами для получения списка рассылки нежелательной почты (фишинга), развертывания фишинговых систем или других комплектов ПО для атаки, получения бот-сети и самостоятельного проведения атак. Также она может вести переговоры с одной стороной или оператором сети услуг fast flux для управления фишинговой атакой от своего имени.

В хостинге fast flux сети услуг fast flux используются для достижения двух целей:

1) **Для размещения перенаправляющих веб-сайтов**. Боты в данной сети услуг обычно не размещают содержимое клиента fast flux, а выполняют перенаправление на веб-сервер, с которого клиент fast flux выполняет несанкционированные или противозаконные действия. Если для хостинга fast flux используется только эта сеть, для описания данной деятельности применяется термин *single flux*.

2) **Для размещения серверов имен**. Боты в данной сети услуг запускают направляющие серверы для клиента fast flux. Эти серверы имен переадресовывают DNS-запросы на скрытые серверы имен, на которых размещены зоны, содержащие записи ресурсов DNS A для набора перенаправляющих веб-сайтов. Скрытые серверы имен не пересылают запросы обратно через направляющий сервер имен, а отправляют ответ непосредственно запрашивающему хосту. Когда для усиления эффекта атаки вместе с сетью (1) используется вторая сеть, для описания данной деятельности применяется термин *double flux*.

[2] См. «Market Activity» (Рыночная деятельность) в *«An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants» (Исследование природы и причин огромного числа случаев взлома систем), см. http://*www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf

Данная структура показана на рисунке 1.

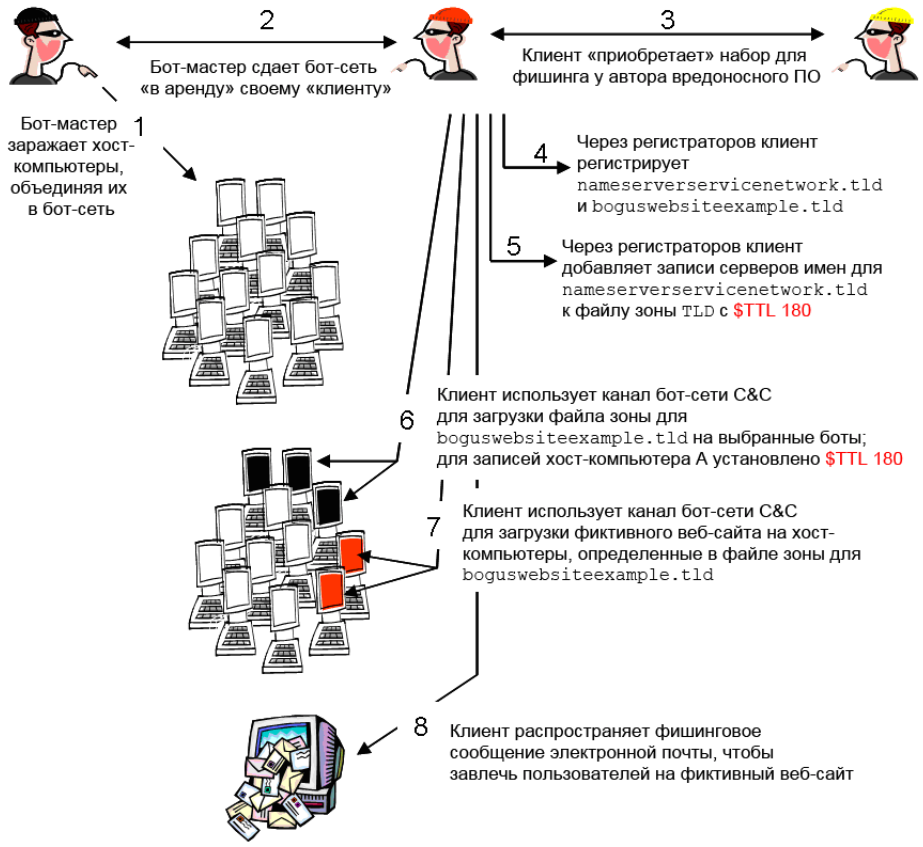

Рисунок 1. Элементы хостинг-атаки double flux

Атака на службу имен: хостинг Double Flux

Клиенты Fast flux часто регистрируют доменные имена для своих противозаконных действий у аккредитованных регистраторов или посредников. В одном из видов атаки предполагается, что клиент fast flux регистрирует доменное имя (для сети услуг flux) для размещения противозаконных веб-сайтов `(boguswebsitesexample.tld)` и одно или несколько доменных имен для сети услуг flux для предоставления услуг преобразования имен `(nameserverservicenetwork.tld)`. Клиент fast flux определяет эти домены для своего оператора сети услуг fast flux. Оператор сети услуг fast flux использует автоматизированные средства быстрого изменения информации сервера имен в регистрационных записях, поддерживаемых для этих доменов регистратором; в частности, оператор сети услуг fast flux

- изменяет IP-адреса доменных серверов имен для указания на другие хосты в домене `nameserverservicenetwork.tld` и
- устанавливает очень маленькое значение времени существования (TTL) в записях адресов для данных серверов имен (обычно от 1 до 3 минут).

Записи ресурсов, связанные с доменом серверов имен, использовавшимся при хостинге fast flux, могут отображаться в файле зоны TLD следующим образом:

```
$TTL 180
boguswebsitesexample.tld.      NS
NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.      NS
NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.   A  10.0.0.1
NS2.nameserverservicenetwork.tld.   A  10.0.0.2
```

Следует отметить, что для записей ресурсов устанавливается очень непродолжительное время существования (TTL) (в данном примере – 180 секунд). По истечении времени существования осуществляется автоматическая замена существующего набора записей A для серверов имен новым:

```
$TTL 180
boguswebsitesexample.tld.      NS
NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.      NS
NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.   A  192.168.0.123
NS2.nameserverservicenetwork.tld.   A  10.10.10.233
```

Поэтому вероятность определения и закрытия серверов имен, поддерживающих данную атаку fast flux, является чрезвычайно малой.

Записи ресурсов в `nameserverservicenetwork.tld` указывают на прокси-серверы или направляющие серверы, а не на боты, предоставляющие разрешение имен для `boguswebsitesexample.tld`. Направляющие серверы используют порт 53 и переадресовывают DNS-запросы на DNS-бот, на котором размещен файл зоны для `boguswebsitesexample.tld`. DNS-бот преобразовывает доменное имя мошеннического веб-сайта в IP-адрес хоста в веб-сети услуг flux и возвращает ответное сообщение непосредственно запрашивающему преобразователю. В данный момент IP-адрес DNS-бота известен только потенциально большому количеству направляющих серверов, при этом IP-адреса направляющих серверов изменяются каждые 180 секунд.

Направляющий веб-хостинг flux

В предыдущем разделе описалась применение ботов в сети `nameserverservicenetwork.tld` и быстрое изменение записей A хостов направляющего веб-сервера в сети `boguswebsitesexample.tld` во избежание обнаружения при использовании хостинга double flux. Для записей ресурсов A направляющих веб-серверов также устанавливаются небольшие значения TTL. По истечении времени TTL веб-серверов автоматической процесс обработки оператора сети услуг fast flux гарантирует замену существующего набора записей A для веб-серверов новым. Поэтому вероятность определения и закрытия направляющих веб-серверов, поддерживающих данную атаку fast flux, является чрезвычайно малой.

Записи, связанные с противозаконным веб-сайтом, могут отображаться в файле зоны, размещенном на DNS-боте в сети `nameserverservicenetwork.tld`, таким образом:

```
boguswebsitesexample.tld.     180  IN   A    192.168.0.1
boguswebsitesexample.tld.     180  IN   A    172.16.0.99
boguswebsitesexample.tld.     180  IN   A    10.0.10.200
boguswebsitesexample.tld.     180  IN   A    192.168.140.11
```

Следует снова отметить, что для каждой записи ресурсов A устанавливается очень маленькое время существования (TTL) (в данном примере – 180 секунд). По истечении данного времени записи ресурсов автоматически изменяются и указывают на других ботов, на которых размещен данный противозаконный веб-сайт. Спустя несколько минут файл зоны может иметь следующий вид:

```
boguswebsitesexample.tld.     180  IN   A    192.168.168.14
boguswebsitesexample.tld.     180  IN   A    172.17.0.199
boguswebsitesexample.tld.     180  IN   A    10.10.10.2
boguswebsitesexample.tld.     180  IN   A    192.168.0.111
```

Сочетание быстрого обновления записей A в зоне `boguswebsitesexample.tld` и записей A сервера имен в зоне TLD чрезвычайно эффективно для поддержания работоспособности незаконных сайтов в течение более длительного периода по сравнению с сайтами, не использующими fast flux.

Хостинг fast flux: связь с тестированием доменных имен

Некоторые специалисты считают тестирование доменных имен и фишинг связанными операциями[3]. Антифишинговая рабочая группа APWG опубликовала отчет, посвященный связи между тестированием доменных имен и фишинговыми атаками. В этом отчете приведена краткая информация о данных, полученных в результате проведения двух исследований, целью которых было определить, используются ли доменные имена сторонами, тестирующими их, для проведения фишинговых атак. Один из членов APWG сначала отобрал набор доменных имен, использовавшихся при проведении фишинговых атак, и попытался определить, отменялись ли эти имена во время дополнительного льготного периода. Другой член APWG сопоставил доменные имена, использовавшиеся при проведении фишинговых атак, с приблизительно тремя миллионами доменных имен, протестированных в течение одной недели. Результаты обоих исследований показали, что «возможные случаи тестирования доменных имен злоумышленниками очень редки, при этом для существующих случаев можно найти другие объяснения, не связанные с тестированием»[4].

В фишинговых атаках все чаще используется хостинг fast flux (особенно в атаках, целью которых являются крупные финансовые учреждения); таким образом, SSAC делает вывод, что между тестированием доменных имен и хостингом fast flux отсутствует взаимосвязь. SSAC также обращает внимание на отличия между целями хостинга fast flux и тестированием доменных имен. Главная цель хостинга fast flux состоит в продлении срока существования сайта, с помощью которого осуществляются противозаконные действия, которые приносят прибыль (включая кражу финансовой информации и данных кредитных карт). Украденные кредитные карточки используются для оплаты услуг регистрации доменного имени фишингового сайта, поэтому регистрация имени и избавление от него являются нецелесообразными. Тестеры доменов, напротив, заинтересованы исключительно во внесении регистрационного взноса для доменных имен, которые окажутся прибыльными в течение нескольких дней испытательного периода.

Текущие и возможные приемы уменьшения угрозы

Для уменьшения угрозы, которую представляет хостинг fast flux, можно применить несколько следующих приемов.

[3] См. «CADNA Background» (Введение в CADNA), http://www.cadna.org/en/index.html
[4] APWG: «The Relationship of Phishing and Domain Name Tasting» (Взаимосвязь между фишинговыми атакми и тестированием доменных имен), http:// www.antiphishing.org/reports/DNSPWG_ReportDomainTastingandPhishing.pdf

Закрытие ботов, на которых размещены средства fast flux

Бот-мастера взламывают компьютеры в персональных и корпоративных сетях. Однако бот-мастер обычно взламывает недостаточно защищенные компьютеры, подключенные к широкополосным каналам связи (кабельным модемам и цифровым абонентским линиям), поскольку вероятность обнаружения взламываемого хоста в них выше, чем в сетях, которыми управляет опытный IT-персонал. Для систем серверов в образовательных, правительственных организациях и на предприятиях также существует угроза взлома, но они, как правило, реже подвергаются атакам, поскольку существует больший риск обнаружения попыток несанкционированного доступа сетевыми администраторами.

Ниже приведено несколько доступных на сегодняшний день методов снижения риска атаки, которые можно широко использовать для уменьшения количества компьютеров, которые могут быть взломаны и использованы для размещения программных ботов:

a) улучшенные меры безопасности настольных компьютеров (антивирусные и антишпионские программы, программы обнаружения несанкционированного доступа, персональный брандмауэр) как в частных, так и общедоступных (например службах с широкополосным доступом) сетях;
~~a)~~b) развертывание шлюзов, фильтрующих вредоносное ПО, поставщиками услуг Интернета для клиентов сетей с широкополосным доступом, поставщиками управляемых служб безопасности или внутренними администраторами систем безопасности для бизнес-сетей, а также активное внедрение шлюзов, фильтрующих вредоносное ПО, администраторами систем безопасности частных сетей;
~~a)~~c) осведомленность, обучение, тренинги с целью достижения понимания и применения строгой политики контроля исходящего трафика.

Formatted: Bullets and Numbering

Существуют также следующие дополнительные методы снижения риска:

d) обрабатываемые и исполняемые списки надежных приложений;
e) управление доступом к сетям;
~~e)~~f) анализ известных поведений бот-сетей, разработка методов обнаружения (например подписи), которые можно использовать для блокировки деятельности на шлюзе безопасности «управления угрозами»; данный прием логически дополняет приведенный выше метод (b).

Formatted: Bullets and Numbering

Хотя методы (a) и (b) кажутся наиболее практичными, их эффективность уменьшения угрозы вредоносного программного обеспечения не доказана. Создатели Storm[5] и подобным образом разработанного вредоносного ПО могут регулярно изменять и распространять данное ПО с помощью новых ботов[6], поэтому методы борьбы с вредоносным ПО, в которых используются подписи, неэффективны при уничтожении вредоносного ПО, например троянского коня Storm[7]. Компьютеры, зараженные этим вредоносным ПО, быстро распространяют вирусы, прежде чем сообщество сможет определить и обезвредить их. Обучение и осведомленность (c) – чрезвычайно медленный процесс. Исследование компьютерной преступности и безопасности, проведенное ЦРУ/ФБР, показывает, что на 97 % компьютеров установлены антивирусные программы, а на 79 % – антишпионские, но уровень заражения ботами угрожающе высок: в июне 2007 г. ФБР объявила, что только в пределах ее юрисдикции в ходе осуществления текущей инициативы по борьбе с бот-сетями было выявлено, что на более чем одном миллионе компьютеров установлены программные боты[8]. Эти цифры относятся к корпоративным сетям и сетям организаций. Пользователи сетей с широкополосным доступом реже используют антивирусные и антишпионские программы, не уделяют должного внимания настройкам безопасности и подключения к сети, а также часто не обновляют подписки на обновления определений вредоносного ПО.

Обрабатываемые и исполняемые списки надежных приложений – это метод предотвращения распространения вредоносного ПО, который запускает исполняемую стратегию; в частности, на компьютере может быть разрешен запуск только надежного набора приложений и связанных процессов. Использование исполняемых списков надежных приложений не является широко распространенным явлением, особенно среди пользователей персональных сетей. Разнообразие приложений, темпы выпуска новых приложений, нехватка ориентированных на потребителя коммерческих предложений и служб, которые можно использовать как надежные источники составления списков надежных приложений, – факторы, препятствующие принятию модели, даже если ею легко управлять.

На сегодняшний день разрабатываются решения по управлению доступом к сетям, направленные на предотвращение создания незащищенных конечных точек, возникающих из-за подключения к локальным и беспроводным локальным сетям. Перед подключением компьютера к Интернету на нем выполняется оценивание уровня безопасности для определения отсутствия вредоносных исполняемых файлов. Если безопасность компьютера нарушена, он изолируется и не может повторно подключиться к сети до устранения угрозы, поскольку сеть с широкополосным доступом (e) не является широко распространенной, и для нее необходимы дополнительные стандарты и ПО. Поставщики услуг Интернета и поставщики услуг доступа к сетям с широкополосным доступом указывают, что они не могут оплатить стоимость внедрения системы фильтрации доступа к сети и входящего трафика, а также управлять ею.

---

[5] «Storm Worm DDoS Attack» (Атаки DDoS типа Storm Worm), http://www.secureworks.com/research/threats/view.html?threat=storm-worm

[6] *«Imperfect Storm aids spammers» (Неудавшиеся спамеры в борьбе против атак типа Storm),* http://www.securityfocus.com/news/11442

[7] Список распространенного вредоносного ПО загрузчика программ-троянов CME-711, http://cme.mitre.org/data/list.html

[8] *«Over 1 Million Potential Victims of Botnet Cyber Crime» (Более одного миллиона людей, ставших потенциальными жертвами интернет-преступлений в бот-сетях),* http://www.fbi.gov/page2/june07/botnet061307.htm

Закрытие хостов fast flux

Большое количество небезопасных серверов, использующихся при подобных атаках, являются компьютерами, подключенными к широкополосным службам. На этих компьютерах обычно размещаются направляющие веб-сайты и программные боты сервера имен.

В настоящее время наиболее часто используемыми процедурами уменьшения угрозы являются обнаружение ошибок, изоляция и ответ. Сначала определяется система, выполняющая противозаконные действия (или направляется соответствующий отчет). В сценарии хостинга fast flux такой системой может быть направляющий веб-сервер, сервер имен или система, в которой размещен противозаконный сайт; лица, отвечающие за борьбу с преступностью, собирают информацию о сайте: расположение и юрисдикция хостинг-системы; владелец домена, администратор сайта и поставщик услуг Интернета; тип противозаконной деятельности. Ответственные лица используют протокол WHOIS и другие средства для параллельного и многократного определения нескольких сторон и обращения к ним, пока им не будет предоставлена помощь в закрытии противозаконной деятельности[9].

- В случаях размещения противозаконных действий во взломанной системе (например, если администратор не знает, что на веб-сервере, на котором проводится законная деятельность, также расположен противозаконный сайт) для содействия ее закрытию обращаются к владельцу домена.
- Обращаются к поставщику услуг Интернета или поставщику услуг хостинга для запроса прекращения размещения данных служб на сервере
- Если ответственные лица нуждаются в локальной помощи (услугах переводчика, подтверждении того, что ответственные лица действуют добросовестно, либо помощи в получении дальнейших сведений), они могут обратиться к локальным службам реагирования на компьютерные угрозы и инциденты (CERT/CIRT). (В некоторых странах службы CERT содействуют скорейшему обращению к ним ответственных лиц).
- В случае обращения к ботам на серверах хост-имен компьютеров, регистраторах или реестрах для удаления записей NS из файлов зон TLD или приостановки работы доменов.

[9] Данный сценарий, относящийся к личной переписке с ответственными лицами, представляет собой образец методов, используемых при ответе на фишинговые атаки для которых интенсивно применяется хостинг fast flux.

Противозаконные сайты могут функционировать со взломанных серверов на законных доменах, предоставляться поставщиками веб-сайтов с услугами совместного хостинга или размещаться на частично законных, «пуленепробиваемых» средствах веб-хостинга[10]. Если сотрудничества добиться не удается (если операторы и местные власти не признают ответственных лиц или не доверяют им, либо не желают действовать на основе информации, предоставляемой ответственными лицами и группами CERT), ответственные лица могут запросить помощь судебных органов (LEA) или добиваться распоряжений суда, чтобы вынудить оператора закрыть сайт. Обычно такие действия предпринимаются только в крайнем случае, так как временные рамки, необходимые для определения судебных органов, сотрудничества с ними и начала судебного иска в соответствующем судебном округе, часто растягиваются на дни и недели, а ответственные лица пытаются добиться закрытия противозаконных сайтов в течение нескольких часов.

Оперативное изменение записей ресурсов A направляющих веб-серверов flux препятствует обнаружению и затрудняет принятие мер для закрытия сайтов fast flux. Во многих случаях срок существования противозаконного сайта, размещенного при помощи fast-flux, намного превышает среднее значение, составляющее около 4 дней[11].

Шаги по улучшению этой формы уменьшения риска включают:

1) внедрение процедур, ускоряющих приостановку работы доменного имени, для устранения проблемы быстрого повторного размещения на другом сервере иного поставщика услуг Интернета закрытых противозаконных сайтов;
2) улучшение взаимодействия и обмена данными между ответственными лицами, судебными органами и службами CERT. Создание баз данных, содержащих контактные данные (на используемых языках), сведения о правовых требованиях, соглашениях и другую информацию, которая может быть полезна при выполнении действий по приостановке.

[10] «Пуленепробиваемый» хостинг связан с поставщиками услуг веб- и массового хостинга электронной почты, которые создают недостаточные условия управления содержанием и деятельностью на серверах или же таковые отсутствуют вообще. Термин «пуленепробиваемые» используется с целью акцентирования внимания том факте, что качество услуг, предоставляемых такими поставщиками, не будет низким. Многие поставщики услуг «пуленепробиваемого» хостинга проводят нечестную политику отношений с судебными органами и организациями, борющимися с преступностью, при этом они осуществляют свою деятельность в судебных округах, местные власти и законы в отношении Интернета которых перелагают относительно тихую гавань для проведения незаконных операций.

[11] Согласно отчету ежемесячной статистики APWG за период с декабря 2006 г. по август 2007 г. среднее время интерактивной работы фишинг-сайтов варьируется в диапазоне от 3,3 по 4,5 дня, см. http://www.apwg.org/phishReportsArchive.html. Однако среднее арифметическое вычисляется без проведения различия между обычными услугами, предоставляемыми фишинг-сайтами и аналогичными, при которых используется fast flux. В связи со стремительными изменениями IP-адресов на хостах fast flux, хостинг fast flux содействовал *снижению* данной оценки.

Удаление доменов, используемых для хостинга fast flux

В некоторых сценариях по закрытию лица, отвечающие за борьбу с преступностью, определяют, что доменное имя используется для атак fast flux, обращаются к регистратору или реестру, в котором оно было зарегистрировано, объясняют суть проблемы и убеждают регистратора удалить доменное имя из службы.

Регистраторы и реестры не обязаны определенным образом реагировать на жалобы, касающиеся хостинга fast flux, который сам по себе не является противозаконной деятельностью, если не установлена его очевидная связь с противозаконной деятельностью (использование компьютера в незаконных целях и компьютерном мошенничестве или кражей личных данных). Реестры и регистраторы самостоятельно устанавливают стратегии касательно употребления в незаконных целях и применяют соответствующие процедуры реагирования. Однако существует несколько распространенных практик. Реестры запрашивают необходимые сведения, доказывающие, что доменное имя явно используется в незаконных целях или для содействия незаконной деятельности, и обычно инициируют собственное расследование. Если собственное расследование реестра подтверждает данные, предоставленные ответственным лицом или истцом, она может предоставить их регистратору записи, который быстро предпримет действия для решения данной проблемы. Собственная стратегия регистратора и ICANN RAA (если применимо к TLD, на котором зарегистрировано доменное имя) влияет на ответ регистратора, который может приостановить функционирование домена (например воспользоваться состоянием удержания HOLD для предотвращения преобразования имени со стороны DNS), приостановить действительность доменного имени и изменить запись регистрации, чтобы подвергнуть сомнению законность доменного имени или засвидетельствовать нарушение политики регистрации, либо приостановить действительность доменного имени и удалить его из зоны. Реестры обычно оперативно реагируют на запросы судебных органов, повестки о явке в суд и распоряжения суда. Многие реестры и регистраторы имеют отделы по борьбе с нарушениями, а доступ к вопросам и ответам и контактным формам часто можно получить с помощью обозревателя. Реестры и регистраторы могут предоставлять подобные вопросы и ответы, а также формы для облегчения и ускорения взаимодействия с судебными органами и лицами, отвечающими за борьбу с преступностью.

Оперативное изменение записей ресурсов A направляющих серверов имен flux препятствует обнаружению и затрудняет принятие мер для закрытия сайтов fast flux.

На сегодняшний день применяются (не повсеместно) следующие методы предотвращения угрозы:

- Установка подлинности контактов перед предоставлением разрешения на внесение изменений в настройки серверов имен.
- Принятие мер для предотвращения автоматического (выполняемого по сценарию) внесения изменений в настройки серверов имен.
- Установка минимального допустимого значения TTL (например 30 минут), достаточного для препятствования элементу double flux хостинга fast flux.
- Внедрение или расширение возможностей систем контроля за использованием в незаконных целях для предоставления отчетов касательно наличия чрезмерного количества изменений в настройках DNS.
- Публикация и применение универсального пользовательского соглашения, запрещающего использование зарегистрированного домена и служб хостинга (DNS, Интернет, почта) для содействия противозаконным или спорным действиям (перечисленным в соглашении).

Предложены дополнительные методы обнаружения и предотвращения, среди них:

- **Изоляция доменных имен (а также установка систем-ловушек для хакеров).** На основе набора подлежащих уточнению критериев обновления сервера имен для приостановки предоставления услуг регистратору для доменных имен, подозревающихся в связи с атакой fast flux. Во время периода приостановки наблюдайте за всеми действиями на учетной записи и попытками обновления записи владельца регистрации, а также заносите их в журнал (записывайте). Благодаря этому расширяется окно анализа ошибок, а у исследователей появляется возможность отслеживания обновлений и определения ботов.

- **Ограничение интенсивности внесения изменений (количество изменений, вносимых за час/день/неделю) в серверы имен, связанные с зарегистрированным доменным именем.** Реестры и регистраторы уже применяют приемы ограничения интенсивности для услуг WHOIS на основе запроса для предотвращения использования в незаконных целях. Определите интенсивность внесения изменений, которая (a) учитывает допустимые применения небольших значений TTL для записей NS в файлах зон TLD, (b) предоставляет аналитикам возможность отслеживания происхождения обновлений и определения ботов, и (c) делает небольшие значения TTL менее эффективными для злоумышленников fast flux.

- **Разграничение «обновления небольших значений TTL» и обычной обработки изменений регистрации.** Рассматривайте запросы на установку значений TTL, не превышающих определенный уровень, как специальные запросы, требующие проверки.

- **Использование доменов, работа которых приостановлена, для обучения клиентов.** Не сразу возвращайте домены, использовавшиеся в противозаконных целях; сначала создайте целевую страницу и направляйте на нее посетителей, объясняя, что данный домен был закрыт, поскольку использовался для противозаконных или спорных действий, а также информируйте пользователей, как можно обнаружить фишинг и другие правонарушения и самим не стать их жертвой.

Полученные данные

SSAC предлагает сообществу рассмотреть следующие полученные данные:

1) Хостинг Fast flux позволяет создать чрезвычайно сложную систему запуска атак, которая активно использует службы разрешения доменных имен и регистрации для содействия противозаконным и спорным действиям.

2) Текущие методы препятствования хостингу fast flux путем обнаружения и закрытия бот-сетей не являются эффективными.

3) Double flux в большей мере препятствует обнаружению и затрудняет принятие мер для закрытия сайтов fast flux.

4) Частое внесение изменений в записи серверов имен (NS) владельцем регистрации доменного имени и наличие небольших значений TTL в записях A сервера имен в файлах зон TLD являются признаками потенциальных случаев злоупотребления службами имен.

5) Меры, предотвращающие автоматическое внесение изменений в сведения DNS и устанавливающие более продолжительные значения TTL для записей A серверов имен в файлах зон TLD, кажутся эффективными, но применяются не повсеместно.

6) Для борьбы с хостингом fast flux и стимулирования дальнейших исследований были предложены дополнительные меры.

Рекомендации

Хостинг Fast flux является серьезной проблемой, которая может затронуть службы имен во всех TLD. SSAC призывает ICANN, реестры и регистраторов рассмотреть практические методы, приведенные в данном документе Advisory, для применения наиболее эффективных методов борьбы с хостингом fast flux, а также принять решение касательно целесообразности их рассмотрения в последующих соглашениях.