электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 02, февраль 2016

УДК 004.056.53

Механизм атаки DNS Rebinding

Соколов М.Н., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Алешин В.А., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
v.aleshin@bmstu.net

Краткий обзор

Атаки DNS Rebinding нарушают правило ограниченного *домена (domain – англ.)* в браузерах и преобразуют их в открытые сетевые *прокси (proxy – англ.).* В статье рассмотрены новые атаки DNS Rebinding, использующие взаимодействие между браузером и его *плагинами (plug-in – англ.*), такими как Flash Player и Java [1]. Эти атаки могут быть использованы для обхода фаерволов и очень ценны для отправки спама и обмана рекламной системы «оплата за клик». Атаки требуют меньше 100$ для того чтобы временно захватить 100000 IP-адресов. Здесь будет показано, что классический способ защиты от этих атак, называемый «DNS pinning» [2], неэффективен в современных браузерах. Основное внимание в этой работе сконцентрировано на создании сильной защиты от DNS Rebinding атак, которая будет защищать современные браузеры: автор предлагает простые в установке *патчи (patch – англ.)* для плагинов, которые представляют большую угрозу, предоставляет защитные инструменты, dnswall, который предотвратит обход фаервола и детально рассматривает два способа защиты: пиннинг *(pining – англ.)* на основе политик и авторизация имени хоста.

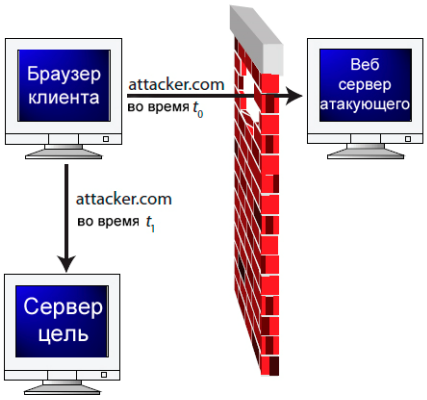
Введение

Люди, которые просматривают веб-страницы, доверяют своему браузеру предотвращение использования своих машин вредоносными веб-сайтами для атак на другие машины. Организации, которые разрешают использование JavaScript и другого *активного контента (active content – англ.)* в фаерволе, полагаются на браузер для

защиты внутренних сетевых ресурсов от атак. Для достижения этих целей в области безопасности, современные браузеры используют правило ограниченного домена, которое пытается изолировать различные «источники», защищая сайты друг от друга.

Атаки DNS Rebinding нарушают правило ограниченного домена, впутывая браузер в объединенные сетевые ресурсы, контролируемые разными объектами в одной сущности, эффективно преобразуя браузеры в открытые прокси. Используя атаку DNS Rebinding, злоумышленник может обойти фаерволы корпоративных сетей, получить доступ к конфиденциальным документам, и эксплуатировать *непропатченные машины (unpatched machines – англ.)* внутри сети. Злоумышленник может так же захватить IP-адрес ни в чем невинных клиентов для рассылки спама, мошенничества с кликами и обвинения клиентов в содеянном. Уязвимость DNS Rebinding позволяет злоумышленнику читать и писать прямо в сетевые *сокеты (socket – англ.)*. Атаки возможны с помощью основанных на JavaScript *ботнет сетях (botnet – англ.)*, которые могут отправлять HTTP запросы, но не могут получать ответы.

Для совершения DNS Rebinding атаки, злоумышленнику необходимо только зарегистрировать доменное имя, например, attacker.com, и привлечь веб-трафик, например, запустив рекламу. В обычной DNS Rebinding атаке, злоумышленник отвечает на DNS запросы для attacker.com IP-адресом собственного сервера с малым временем жизни (TTL) и запускает у клиентов вредоносный JavaScript. Чтобы обойти фаервол, когда *скрипт (script – англ.)* отправляет второй запрос на attacker.com, злоумышленник меняет привязку имени хоста на IP-адрес сервера-цели, который недоступен из публичного интернета. Браузер считает, что два сервера принадлежат одному и тому же домену, потому что они разделяют имя хоста, и это позволяет скрипту прочитать ответ сервера. Скрипт может с легкостью прочитать ответ, что позволяет злоумышленнику читать произвольные документы на внутреннем сервере, как показано на рисунке.



Для совершения этой атаки, злоумышленник не ставил под угрозу какой-либо DNS-сервер. Он просто предоставил действительный ответ для attacker.com, домена принадлежащего злоумышленнику. Эта атака очень отличается от "фарминга", где злоумышленник должен скомпрометировать имя хоста принадлежащего цели на нарушение DNS кэша пользователя или сервера. DNS Rebinding не требует такой подрывной деятельности. Следовательно, DNSSEC не обеспечивает защиты от DNS Rebinding'a: злоумышленник может на законных основаниях подписывать все DNS записи, предоставленные с его или ее сервера DNS во время атаки.

Атаки DNS Rebinding были известны последний десяток лет. Общая защита, реализованная в нескольких браузерах - DNS pinning: как только браузер распознает IP-адрес из имени хоста, браузер кэширует результат на фиксированное время, независимо от TTL. В результате, когда JavaScript подключается к attacker.com, браузер будет подключаться к серверу злоумышленника, вместо внутреннего сервера.

Пиннинг уже неэффективная защита от DNS Rebinding атак в современных браузерах из-за уязвимостей внутри плагинов. Эти плагины обеспечивают дополнительный функционал, в том числе доступ к сети на уровне сокетов. Браузер и каждый плагин поддерживает разные базы данных связок, создавая новый класс уязвимостей, который мы называем *мульти-пин уязвимости (multi-pin vulnerabilities – англ.)*, которые позволяют злоумышленнику использовать DNS Rebinding атаки.

Эти атаки не требуют от пользователей нажатия на какие-либо вредоносные ссылки: пользователю нужно только просмотреть рекламу атакующего. Потратив меньше, чем $ 100 на рекламу, злоумышленник может захватить 100000 уникальных IP-адресов для рассылки спама, совершения мошенничества с кликами, или использовать их как открытые сетевые прокси-сервера.

Доступ к сети в браузере

Для отображения веб-страниц, браузеры делают сетевые запросы по *статическому контенту (static content – англ.)*, такому как HTML и по активному контенту, такому как JavaScript, Flash Player, Java и CSS. Браузеры ограничивают этот сетевой доступ для того, чтобы предотвратить вредоносные сетевые подключения с веб-сайтов.

Правило ограничения домена обеспечивает частичную изоляцию ресурсов путем ограничения доступа по происхождению, с указанием, когда контент из одного источника может получить доступ к ресурсу в другом источнике. Правило применяется как к сетевому доступу, так и к состояниям браузера, таким как интерфейс Document Object Model (DOM), *куки (cookies – англ.), кэш (cache – англ.),*

история, и база данных паролей [3]. Атаки, описанные в этой статье, обходят правило ограничения домена для сетевого доступа.

Уязвимости DNS Rebinding

Политика сетевого доступа в веб-браузерах на основе имен хостов, связывает систему доменных имен (DNS) с IP-адресами. Злоумышленник, использующий DNS Rebinding, пытается нарушить эту политику безопасности с помощью связывания его или ее имени хоста, и с атакующим сервером, и с сервером-целью.

- **Стандартные уязвимости DNS Rebinding**

Стандартные атаки DNS Rebinding используют единые технологии браузера (например, JavaScript, Java или Flash Player) для подключения к нескольким IP-адресам с одним именем хоста.

Множественные А-записи. Когда клиент переводит имя хоста, используя DNS, сервер может отвечать несколькими А-записями, указывающими IP-адреса хоста. Первая атака с использованием DNS Rebinding в 1996 году изменила это свойство для запутывания политики безопасности Java Virtual Machine (JVM):

1. Клиент посещает вредоносный веб-сайт attacker.com, содержащий *Java-апплет (Java-applet – англ.).* DNS-сервер злоумышленника связывает attacker.com с двумя IP-адресами: веб-сервером злоумышленника и веб-сервером цели.

2. Клиент выполняет апплет злоумышленника, который открывает сокет к цели. JVM разрешает это соединение, поскольку IP-адрес цели содержится в записи DNS для attacker.com.

Текущие версии JVM не подвержены этой атаке, поскольку политика безопасности Java была изменена. Апплетам теперь запрещено подключаться к IP-адресам, с которых они были загружены

В JavaScript версии этой атаки, злоумышленник посылает JavaScript браузеру, который предписывает браузеру, подключится обратно на attacker.com. Сервер злоумышленника отказывает во втором соединении TCP, заставляя браузер переключиться на IP-адрес жертвы. Последующие запросы XMLHttpRequest, вызванные из кода злоумышленника будет подключаться к новому IP адресу.

Динамический DNS. В 2001 году была проведена оригинальная атака на Java, с использованием динамического DNS:

1. Клиент посещает вредоносный веб-сайт attacker.com, содержащий JavaScript. Сервер DNS-атакующего настроен так, чтобы связать attacker.com и IP злоумышленника с очень короткой TTL.

2. Злоумышленник связывает attacker.com с IP адресом цели.

3. Вредоносный скрипт использует XMLHttpRequest, для подключения к attacker.com, который теперь переводится в IP-адрес сервера цели.

Из-за того что соединение в шаге 3 имеет то же имя хоста, что и исходный вредоносный скрипт, браузер позволяет злоумышленнику прочитать ответ от цели.

Пиннинг в современных браузерах. Текущие браузеры защищаются против стандартных атак DNS Rebinding «закрепляя» имя хоста к IP-адресу, предотвращая ссылки имен хостов на несколько IP-адресов.

- **Мульти-пин уязвимости**

Современные браузеры используют несколько плагинов для визуализации веб-страниц, многие из которых дают прямой доступ к сокетам источника. Другой класс Rebinding атак использует тот факт, что различные технологии содержат различные DNS базы данных привязок. Если одна технологии привязывается к IP-адресу атакующего, а другая к IP-адресу цели, злоумышленники могут воспользоваться связью между технологиями для обхода правила одного домена.

Атаки с использованием DNS Rebinding

Злоумышленник может использовать уязвимости DNS Rebinding для создания некоторого числа атак. Для некоторых из этих атак, злоумышленнику требуется прямой доступ к сокетам, обеспечиваемый DNS связыванием с помощью Flash Player и Java, в то время как другим атакам требуется только умение читать HTTP ответы от цели. Атаки делятся на две большие категории, в соответствии с целью злоумышленника:

1. *Обход фаервола*. Злоумышленник может использовать DNS Rebinding для доступа к машинам, защищенным фаерволом, к которым он или она не может получить доступ напрямую. С прямым доступом к сокетам, злоумышленник может взаимодействовать с рядом внутренних сервисов, не относящихся к HTTP.

2. *Захват IP*. Злоумышленник также может использовать DNS Rebinding для доступа к публичным серверам с IP адреса клиента. Это позволяет злоумышленнику воспользоваться преимуществами явного или неявного доверия цели к IP адресу клиента.

Для проведения этих атак, злоумышленник должен сначала убедить клиента загрузить какой-нибудь активный контент. После загрузки на машину клиента, код злоумышленника может общаться с любой машиной доступной клиенту.

Защита от Rebinding'a

Защита от DNS Rebinding атак может быть реализована в браузерах, плагинах, DNS преобразователях, межсетевых экранах и серверах. Эта защита варьируется от сложности разработки, сложности развертывания и эффективности против обхода фаервола и захвата IP. В дополнение к необходимым мерам снижения риска для Flash Player, Java LiveConnect и браузеров, возможны три метода защиты:

1. *Решение обхода фаервола.*

Сети могут быть защищены от обхода фаервола путем запрета перевода внешних имен хостов к внутренним IP-адресам, запрещая злоумышленнику назвать целевой сервер. Не имея возможности назвать цель, злоумышленник не сможет совместить целевой сервер с доменом под его контролем. Эти вредоносные связки могут быть заблокированы либо путем фильтрации пакетов в фаерволе, либо путем изменения преобразователей DNS, используемых клиентами в сети.

Блокирование перевода внешних имен на внутренние адреса предотвращает обход фаервола, но не защищает от захвата IP. Злоумышленник все еще может использовать внутренние машины для атаки на сервисы, работающие в общедоступном Интернете.

2. *Исправление плагинов*

Плагины – особый источник сложности в защите против DNS Rebinding атак, потому что обеспечивают доступ к сети на уровне сокетов, и работают независимо от браузеров. Для того чтобы предотвратить атаки DNS Rebinding, эти плагины должны быть пропатчены.

3. *Исправление браузеров*

Делится на две категории:

- *Пиннинг на основе политик.* Предлагается поддерживаемая серверами политика, для определения, когда можно безопасно пересвязать имя хоста, с одного IP-адреса на другой, обеспечивая надежность без снижения безопасности. Для безопасной пересвязки, браузер должен получить политику, как со старого, так и с нового IP-адреса (потому что некоторые атаки сначала привязываются к атакующему, тогда как другие сначала привязываются к цели). Серверы могут расположить эту политику в хорошо известном месте, таком как файл /crossdomain.xml, или в обратном DNS.

- *Авторизация имени хоста.* В Интернете, клиентам требуется дополнительная информация для определения набора действительных имен хостов для данного IP-адреса. Предполагается, что серверы объявляют набор имен хостов, который они считают для себя действительным и клиенты проверяют эти объявления перед привязкой имени хоста к IP адресу, чтобы определить, на какие имена хостов могут отображаться IP-адреса.

Заключение

В статье рассмотрена уязвимость, позволяющая злоумышленнику получить доступ к конфиденциальным данным организаций. Данная уязвимость делится на две категории: стандартная уязвимость и мульти-пин уязвимость. Также приведен механизм создания ботнет сети, предоставляющей возможность злоумышленнику захватить более 1000 IP-адресов и остаться при этом незамеченным.

Эти уязвимости могут быть устранены тремя способами: защита от обхода фаервола, установка патчей для плагинов, изменение поведения браузеров. Так как данная уязвимость может нанести серьезный урон предприятию необходимо уделить особое внимание механизмам ее устранения.

Список литературы

[1]. Jackson C., Barth A., Bortz A., Shao W., Boneh D. Protecting Browsers from DNS Rebinding Attacks // 14th ACM Conference on Computer and Communications Security (Alexandria, VA, USA, October 29–November 2, 2007): proceedings. Alexandria, VA, USA, 2007. P. 421–431.

[2]. Johns M., Lekies S., Stock B. Eradicating DNS rebinding with the extended same-origin policy // 22nd USENIX Security Symposium (Washington, D.C., USA, August 14–16, 2013): proceedings. Washington, D.C., USA, 2013. P. 621–636.

[3]. Jackson C., Bortz A., Boneh D., Mitchell J. Protecting browser state from web privacy attacks // The 15th International World Wide Web Conference (Edinburgh, Scotland, May 23–26, 2006): proceedings. Edinburgh, Scotland, 2006. P. 737–744.