СЛАБЫЕ СТОРОНЫ ТЕХНОЛОГИИ WPAD

Сергей Рублев
Эксперт по информационной безопасности "Positive Technologies"
(srublev@ptsecurity.ru)

МОСКВА 2009

ОГЛАВЛЕНИЕ

1 ВВЕДЕНИЕ 3

2 ОБЗОР WPAD 4

2.1 Сценарии Proxy Auto Configuration 4

2.2 Принцип работы WPAD в корпоративной сети 6

3 СЦЕНАРИИ АТАК НА WEB PROXY AUTO DISCOVERY 7

3.1 Атака с использованием DNS-сервера 7

3.2 Атака с использованием WINS-сервера 9

3.3 Атака в доступной подсети 10

4 ИСПОЛЬЗОВАНИЕ WPAD В СЛУЖБАХ MICROSOFT 12

5 УСТРАНЕНИЕ «УЯЗВИМОСТИ РЕГИСТРАЦИИ WPAD» ОТ MICROSOFT 13

6 РЕКОМЕНДАЦИИ ПО УСТРАНЕНИЮ УЯЗВИМОСТИ 15

6.1 Для конечных пользователей: 15

6.2 Для системных администраторов 15

7 ВЫВОДЫ 16

8 ЛИТЕРАТУРА 17

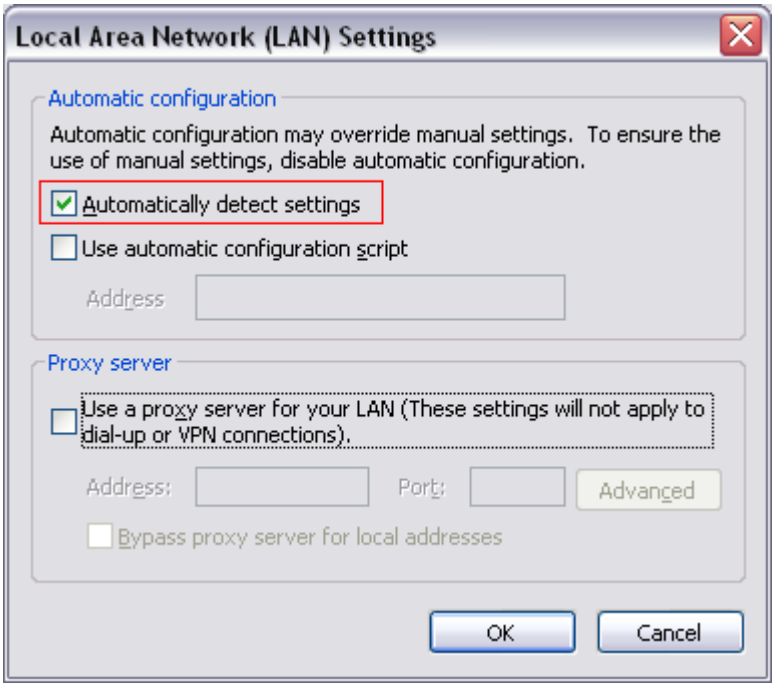
1 Введение

В процессе анализа ежемесячных обновлений от Microsoft мое внимание привлек бюллетень MS09-008, а точнее, его часть, в которой фигурирует имя WPAD. Этот бюллетень исправляет целый ряд уязвимостей в службах Microsoft DNS и Microsoft WINS, среди которых значится «Уязвимость регистрации WPAD», однако данное имя не первый раз встречается в уведомлениях по безопасности. Впервые о слабых сторонах WPAD заговорили в 1999 г., в 2007 г. был опубликован широкий спектр проблем, связанных с этой технологией, в том же году на конференции ShmooCon 2007 Крис Пейджет (Chris Paget) представил практические примеры эксплуатации уязвимостей WPAD. Сейчас, спустя 10 лет, Microsoft продолжает выпускать заплатки, закрывающие бреши данной технологии, а вопрос о безопасности сетей, в которых применяется WPAD, так и остался открытым. Успешная атака на WPAD гарантирует злоумышленникам полный контроль над пользовательскими данными, передаваемыми в Интернет, что может привести к краже критической информации, такой как пароли или номера банковских карт. На потенциальную опасность WPAD во многом влияют два фактора: во-первых, использование в конфигурации «по умолчанию», во-вторых, слабая осведомленность рядовых пользователей в данном вопросе.

В этой статье мы поговорим об архитектуре WPAD и основных принципах функционирования данной технологии в корпоративных и домовых сетях, рассмотрим реальные примеры атак, а также разработаем рекомендации для рядовых пользователей и системных администраторов, позволяющие обезопасить себя от действий злоумышленников.

2 Обзор WPAD

WPAD (Web Proxy Auto Discovery) – протокол, позволяющий Web-клиентам автоматически определять местоположение файла настроек браузера для работы через прокси-сервер. В 1999 г. Microsoft представила данный протокол на рассмотрение в IETF, однако в качестве стандарта WPAD так и не был принят. В настоящее время WPAD поддерживается семейством браузеров Internet Explorer и Mozilla Firefox (Google Chrome и Apple Safari используют настройки прокси-серверов браузера Internet Explorer, т.е. также поддерживают WPAD). Поддержка WPAD присутствует и в семействе открытых операционных систем, например, в браузере Konquerror в ОС Linux.



Включение WPAD в Microsoft Internet Explorer

WPAD – это протокол обнаружения в сети специального файла (сценария). В спецификации WPAD перечислены способы и протоколы, с помощью которых осуществляется поиск. Для понимания технологии WPAD необходимо более детально познакомиться со сценариями автоматической настройки браузеров.

2.1 Сценарии Proxy Auto Configuration

Файл Proxy Auto Configuration (далее PAC-файл) используется в корпоративных сетях для централизованного распространения настроек, которые применяются при работе через прокси-сервер для браузеров пользователей.
По сути PAC представляет собой сценарий на языке JavaScript.

В нем должна быть определена функция FindProxyForURL(url, host), где
url – запрашиваемый адрес;
host – часть url в формате «имя хоста:порт».

Пример PAC файла:

```
function FindProxyForURL(url, host)
{
     return "PROXY proxy.example.com:8080; DIRECT";
}
```

Этот конфигурационный файл дает указание браузеру использовать прокси-сервер proxy.example.com для получения всех Web-страниц. Более подробное описание синтаксиса PAC-файлов можно найти в [3].

PAC-файлы могут использоваться как совместно с WPAD, так и обособленно, в этом случае в Интернет-браузере необходимо явно указать сетевой путь к данному файлу.

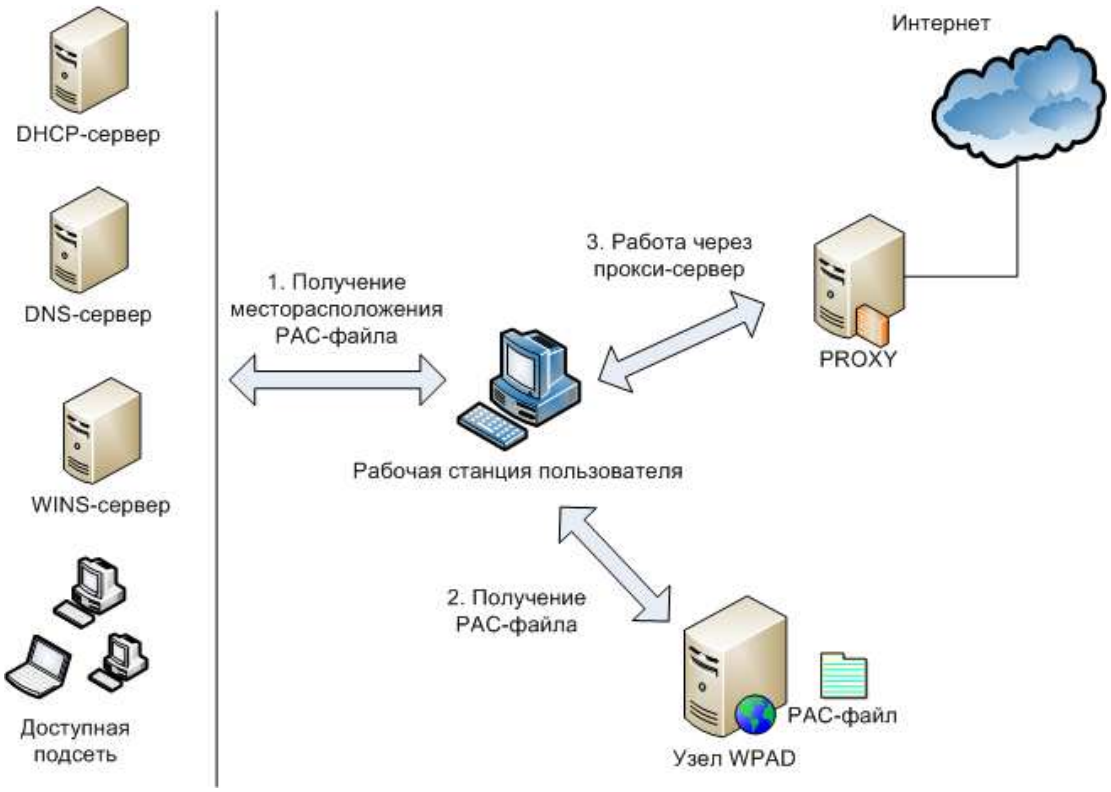
WPAD предоставляет пользователю возможность получения месторасположения PAC-файла одним из следующих способов:

- от DHCP-сервера;
- запрос к DNS-серверу;
- запрос к WINS-серверу;
- широковещательный запрос NetBIOS Name;
- локальный файл hosts;
- локальный файл lmhosts.

При использовании WPAD к PAC-файлу предъявляются следующие требования:

- PAC-файл должен располагаться в корневой папке, опубликованной на Web-сервере;
- PAC-файл должен иметь имя wpad.dat.

2.2 Принцип работы WPAD в корпоративной сети



Принцип работы WPAD

- Администратор создает специальный файл конфигурации (PAC-файл);
- Администратор резервирует WPAD- имя для сетевого узла, на котором настраивает Web-сервер, доступный по порту 80/tcp. В корневой каталог Web-сервера помещается PAC-файл с именем wpad.dat;
- Браузер клиента получает месторасположение PAC-файла;
- Браузер считывает содержимое файла, используя HTTP-запрос;
- Браузер выполняет настройку параметров работы через прокси-сервер.

3 Сценарии атак на Web Proxy Auto Discovery

В Internet Explorer WPAD включен по умолчанию, что делает уязвимым к атакам огромное число пользователей, отдающих предпочтение данному браузеру, а также браузерам, импортирующим его настройки. По данным SpyLog за апрель 2009 г. Internet Explorer, Apple Safari и Google Chrome вместе используют 55% пользователей Рунета..

Наиболее уязвимым местом в технологии WPAD является поиск месторасположения PAC-файла. Если злоумышленнику удается убедить клиента в том, что необходимый файл конфигурации находится на сетевом узле, подконтрольном атакующему, атаку можно считать состоявшейся.

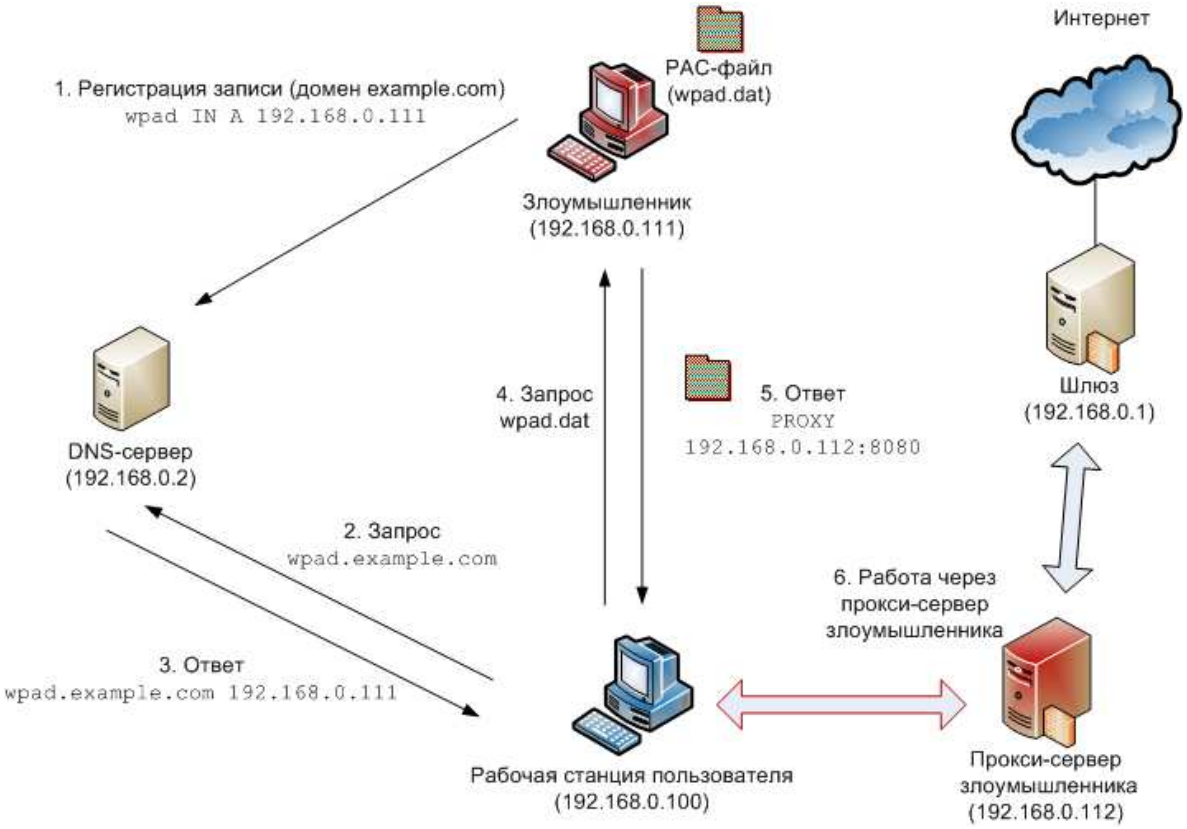
Для успешной атаки злоумышленнику необходимо иметь:

1. Подконтрольный Web-сервер для расположения на нем PAC-файла;
2. Подконтрольный прокси-сервер;
3. Инструменты для контроля трафика, состав которых выбирается исходя из поставленных задач, например: перехватчик SSL-сессий, анализатор сетевых пакетов и т.д.

В рамках данной статьи не будут рассматриваться атаки, основанные на внедрении в сеть ложного DHCP-сервера, так как такая атака позволяет полностью контролировать все настройки сетевой подсистемы клиента, в том числе и WPAD. Далее по тексту предполагается, что месторасположение PAC-файла в данной сети по DHCP не распространяется. Локальные файлы hosts и lmhosts будем считать недоступными для злоумышленника.

3.1 Атака с использованием DNS-сервера

Система DNS поддерживает динамические обновления записей, что позволяет клиентам автоматически регистрировать свои имена и IP-адреса на DNS-сервере при входе в сеть или изменении IP-адресов с помощью сервера DHCP. Если в атакуемой зоне разрешены неаутентифицированные динамические обновления, то для регистрации записи достаточно одного специального DNS-пакета.



Сценарий атаки с использованием DNS-сервера

На схеме показан общий случай, во время атаки прокси-сервер злоумышленника и точка распространения PAC-файлов может находиться на одном и том же сетевом узле.

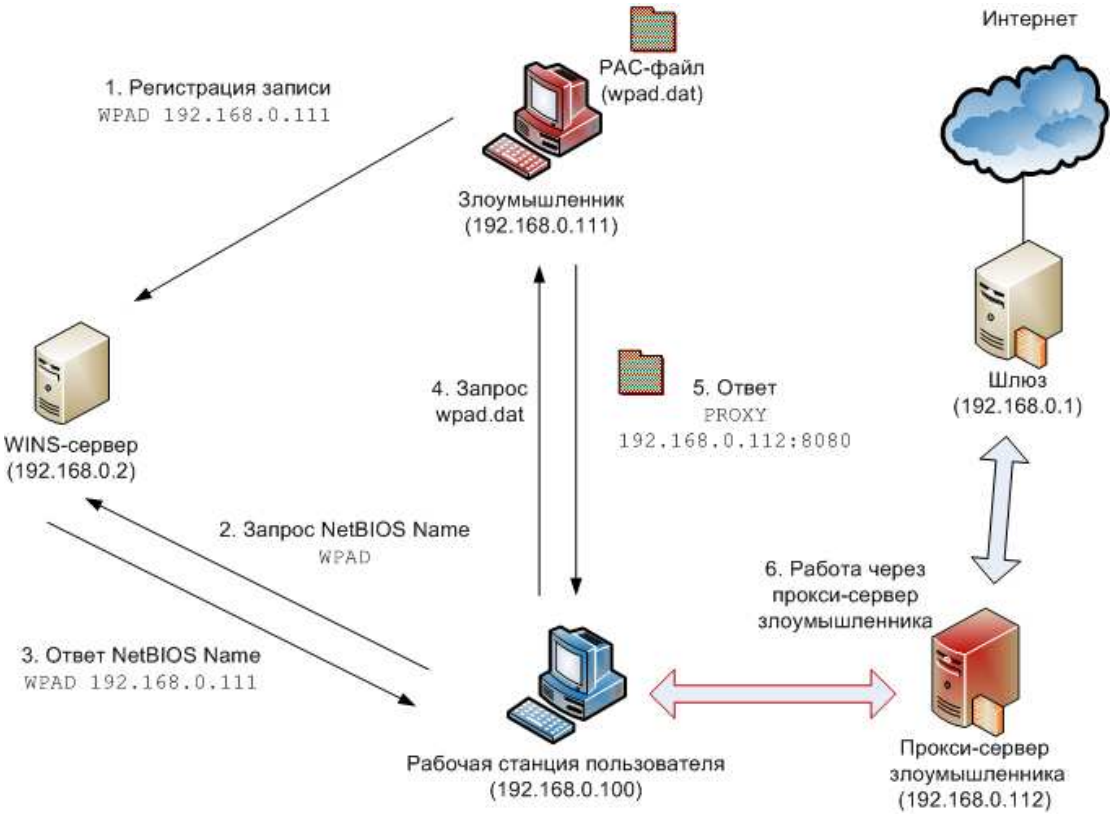
1) Злоумышленник регистрирует на DNS-сервере следующую запись: wpad.<атакуемый домен> IN A <IP-адрес злоумышленника>.
2) Клиент запрашивает у DNS-сервера IP-адрес узла с именем wpad.<домен>;
3) DNS-сервер в ответ на этот запрос возвращает IP-адрес злоумышленника;
4) Клиент запрашивает PAC-файл (wpad.dat);
5) Клиент настраивает браузер в соответствии с PAC-файлом;
6) Далее весь трафик клиента проходит через прокси-сервер, контролируемый злоумышленником.

Примечания: Если DNS-сервер работает в составе домена Active Directory, возможна более безопасная конфигурация, позволяющая динамическое обновление записей только для аутентифицированных пользователей. Для успешной атаки в этом случае злоумышленнику необходимо иметь корректную учетную запись в атакуемом домене. [4]

Данный класс атак актуален только в сетях, имеющих доменную структуру, так как в сети на базе рабочих групп поиск PAC-файла при помощи запроса к DNS-серверу не используется. Атакам, описанным далее, подвержены как доменные, так и одноранговые сети.

3.2 Атака с использованием WINS-сервера

Регистрация имен компьютеров, входящих в сеть, является штатной функцией WINS-сервера. Как и в случае с DNS-сервером регистрация осуществляется при помощи одного специального пакета.



Сценарий атаки с использованием WINS-сервера

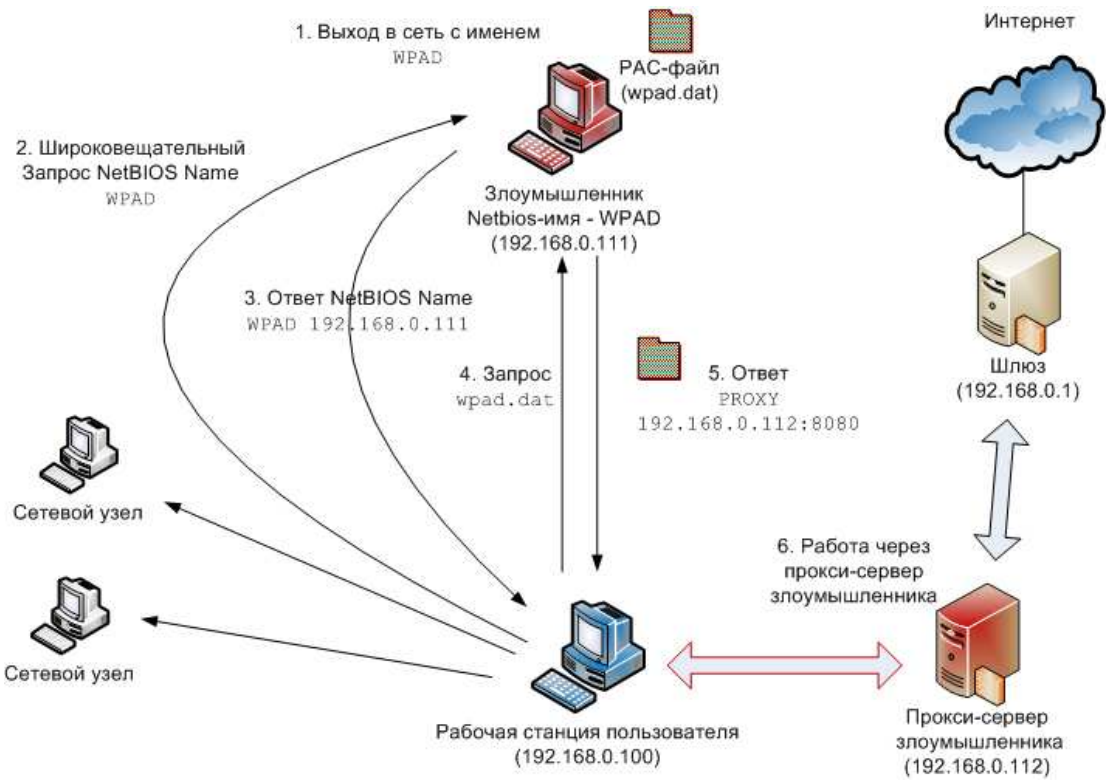
1) Злоумышленник регистрирует на WINS-сервере следующую запись:
2) WPAD <IP-адрес злоумышленника> (тип записи Unique)
3) Клиент запрашивает от WINS-сервера IP-адрес узла с NetBIOS-именем WPAD;
4) WINS-сервер в ответ на этот запрос возвращает IP-адрес злоумышленника;

5) Клиент запрашивает PAC-файл (wpad.dat);
6) Клиент настраивает браузер в соответствии с PAC-файлом;
7) Далее весь трафик клиента проходит через прокси-сервер, контролируемый злоумышленником.

3.3 Атака в доступной подсети

Если месторасположение PAC-файла не найдено путем запроса к DNS- или WINS-серверам, согласно стандарту WPAD Web-клиенты делают широковещательный NetBIOS-запрос имени WPAD по всей подсети согласно сетевой маске.

Данный вектор атаки доступен, если у злоумышленника есть физический доступ к подсети клиента.



Сценарий атаки в доступной подсети

1) Злоумышленник входит в сеть с NetBIOS-именем WPAD ;
2) Клиент выполняет широковещательный запрос имени WPAD;

3) Злоумышленник посылает в ответ на запрос свой IP-адрес;
4) Клиент запрашивает PAC-файл (wpad.dat);
5) Клиент настраивает браузер в соответствии с PAC-файлом;
6) Далее весь трафик клиента проходит через прокси-сервер, контролируемый злоумышленником.

Описанный выше класс атак легко реализуется в большинстве сетей, где отсутствует строгая политика безопасности. Как пример можно привести домовые сети, сети небольших провайдеров, WiFi-интернет в кафе и торговых центрах, где WINS-серверы не используются, а NetBIOS-трафик не фильтруется на сетевых устройствах.

4 Использование WPAD в службах Microsoft

Помимо браузеров технологию WPAD для поиска прокси-сервера используют и ряд системных компонентов Microsoft:

- служба Windows Update. Данная служба задействует WPAD в момент поиска доступной точки распространения обновлений Microsoft;
- Microsoft Crypto API. При попытке получить обновления списка отозванных сертификатов (CRL - Certificate revocation list) или списка корневых удостоверяющих центров (Root CA – Root Certificate Authority) Crypto API также использует WPAD.

Эти службы задействуют WPAD всегда независимо от настроек Internet Explorer.

Примечание: Windows Update и Crypto API передают только подписанные данные, поэтому не подвержены атакам класса «человек посередине». При организации одной из приведенных выше атак можно вызвать некорректную работу данных служб.

- Microsoft Firewall client for ISA server. При определенной настройке данное приложение выполняет поиск ISA-сервера путем запроса имени wpad от DNS-сервера.

5 Устранение «Уязвимости регистрации WPAD» от Microsoft

В бюллетене MS09-008 исправляются следующие уязвимости:

- DNS Server Vulnerability in WPAD Registration (CVE-2009-0093);
- WPAD WINS Server Registration Vulnerability (CVE-2009-0094).

Несмотря на название, установка исправлений не вносит никаких изменений в сам процесс регистрации имен, некоторые коррективы вносятся только в процесс разрешения (resolving) DNS- и NetBIOS-имени соответственно. До поиска в базе DNS- и WINS-серверы выполняют поиск запрашиваемого имени по «черному списку». Если имя находится в списке, то клиенту возвращается код ошибки «имя не найдено», иначе продолжается штатная работа сервера. Внедрение «черных списков» только сужает потенциальный масштаб атаки, а именно, возможность использования злоумышленником собственных записей на DNS- и WINS-сервере, однако атака на доступную подсеть все равно может быть реализована. Специалисты Microsoft объясняют такое поведение заботой о клиентах, которые внедрили и активно используют технологию WPAD.

«Черные списки» хранятся в следующих ключах реестра:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\GlobalQueryBlockList;
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WINS\Parameters\QueryBlockList.

Состав «черных списков» по умолчанию:
Для DNS-сервера - «wpad isatap»;
Для WINS-сервера - «WPAD WPAD. ISATAP».

Обратите внимание, что если на момент установки исправления в базе WINS или DNS существовали некоторые из вышеперечисленных записей, то они не добавляются в указанные списки.

«Черные списки» распространяются только на динамические записи, таким образом, у администратора есть возможность организовать работу WPAD путем регистрации статической записи в базах DNS и WINS соответственно.

Примечание: динамические записи добавляются в базу DNS- и WINS-сервера с помощью специального запроса регистрации, а статические – через консоль управления сервером.

Рассмотрим чуть подробнее имена, добавляемые в «черные списки». Именам WPAD посвящена вся данная статья. WPAD. (WPAD с точкой) используется компонентами Windows Updates и Crypto API, а ISATAP запрашивается для поиска маршрутизаторов, поддерживающих одноименный протокол. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) - протокол туннелирования пакетов IPv6 в пакетах IPv4, используемый для связи сегментов сети IPv6 через сегмент IPv4. Атаки с использованием имени ISATAP в статье не рассматриваются ввиду малой распространенности протокола IPv6.

6 Рекомендации по устранению уязвимости

6.1 Для конечных пользователей:

- Отключить поддержку WPAD в настройках браузера;
- Указать точку распространения PAC-файла в настройках браузера, если в сети используется конфигурирование настроек прокси-серверов через PAC-файл, и его месторасположение заранее известно.

6.2 Для системных администраторов

В силу специфики уязвимостей более подверженными атакам являются сети, не использующие Web Proxy Auto Discovery, чем сети, где WPAD штатно работает. Для повышения уровня защищенности сети можно предпринять следующие действия:

- Внедрить поддержку WPAD;
- Зарезервировать имена WPAD и WPAD. при помощи статических записей в DNS и WINS, например, для IP-адреса 0.0.0.0. Сервер Microsoft WINS не позволяет регистрировать имена для некорректных IP-адресов, однако, Крис Пейджет (Chris Paget) описал способ, который позволяет обойти это ограничение: можно зарезервировать имя для корректного IP-адреса, а затем изменить этот IP-адрес на 0.0.0.0.

В домене Active Directory существуют способы дополнительного повышения уровня безопасности:

- Разрешить только аутентифицированные обновления записей на DNS-сервере;
- Распространять месторасположение PAC-файла через групповую политику.

7 Выводы

Основным фактором, делающим атаки на WPAD такими опасными, является его повсеместное использование в конфигурации «по умолчанию». В настоящее время корпорация Microsoft активно пропагандирует подход Secure by Default (безопасность по умолчанию) как один из основополагающих принципов SDL (Security Development Lifecycle – цикл разработки безопасных приложений), однако конфигурация прокси-серверов в Internet Explorer служит ярким примером нарушения данного принципа.

О слабых сторонах протокола WPAD известно еще с 1999 года, однако он продолжает использоваться и по сей день. Во многом на это повлияло доминирующее положение Microsoft на рынке Интернет-браузеров, и даже отсутствие стандартизации не смогло приостановить распространение данной технологии.

В статье описаны лишь самые простые атаки на WPAD, но существуют и более трудоемкие, требующие от атакующего дополнительных мер по противодействию средствам защиты. Подмена IP-адреса в пакетах регистрации или временный вывод из строя корпоративного DNS-сервера может помочь обойти ряд ограничений по эксплуатации уязвимости. Выбирая защитные механизмы, сетевым администраторам необходимо учитывать существование довольно большого спектра возможных векторов атаки, а также тот факт, что исправления от Microsoft закрывают уязвимость лишь частично.

Слабые места в использовании WPAD до сих пор не устранены, а значит, у злоумышленников есть широкий простор для атакующих действий.

Возможно, пока вы читаете эту статью, ваш браузер ищет по сети волшебное имя WPAD ☺

8 Литература

1. Доклад Криса Пейджета (Chris Paget) на конференции ShmooCon 2007
   http://video.google.com/videoplay?docid=-4596414840866123044
2. Описание WPAD на Википедии
   http://en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol
3. Примеры PAC-файлов
   http://www.lissyara.su/?id=1717
4. Динамические обновления DNS-зон в Windows 2003 Server
   http://support.microsoft.com/kb/816592
5. Порядок разрешения имен
   http://ru.tech-faq.com/understanding-netbios-name-resolution.shtml
6. Изменения в работе WINS-сервера после установки обновления
   http://support.microsoft.com/kb/968731
7. Описание ISATAP на Википедии
   http://en.wikipedia.org/wiki/ISATAP
8. Обеспечение безопасности DNS для Windows
   http://www.oszone.net/5692/DNS_Windows
9. Уязвимость Web Proxy Auto-Discovery (Microsoft Security Advisory)
   http://www.microsoft.com/technet/security/advisory/945713.mspx
10. Уязвимость WPAD Spoofing (Microsoft Security Bulletin)
    http://www.microsoft.com/technet/security/bulletin/ms99-054.mspx
11. Уязвимость регистрации WPAD (Microsoft Security Bulletin)
    http://www.microsoft.com/technet/security/Bulletin/MS09-008.mspx
12. Утилита компании Positive Technologies по обнаружению потенциально опасных записей в серверах имен DNS и WINS.
    http://www.securitylab.ru/news/379618.php
13. Черновик стандарта WPAD
    http://www.cam.ac.uk/cs/webcache/draft-cooper-webi-wpad-00.txt