WPAD TECHNOLOGY WEAKNESSES

Sergey Rublev
Expert in information security, "Positive Technologies"
(srublev@ptsecurity.ru)

MOSCOW 2009

POSITIVE / TECHNOLOGIES®

CONTENTS

1 INTRODUCTION 3

2 WPAD REVIEW 4

2.1 PROXY AUTO CONFIGURATION SCRIPTS 4

2.2 WPAD IN CORPORATE NETWORK 6

3 WEB PROXY AUTO DISCOVERY ATTACK SCENARIOS 7

3.1 ATTACKS BASED ON DNS SERVER USAGE 7

3.2 ATTACKS BASED ON WINS SERVER USAGE 9

3.3 ATTACK IN AVAILABLE SUB NETWORK 10

4 WPAD IN MICROSOFT SERVICES 12

5 HOW TO FIX WPAD REGISTRATION VULNERABILITY 13

6 RECOMMENDATIONS HOW TO FIX THE VULNERABILITY 14

6.1 FOR END USERS 14

6.2 FOR SYSTEM ADMINISTRATORS 14

7 CONCLUSIONS 15

8 ABOUT ME 16

9 ABOUT POSITIVE TECHNOLOGIES 17

10 LINKS 18

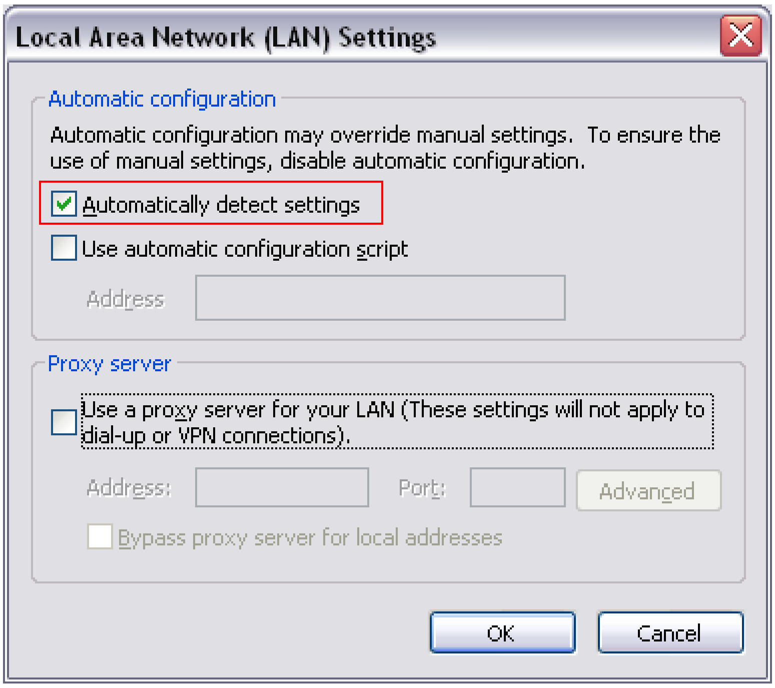
1 Introduction

While reviewing the monthly updates from Microsoft, my attention was attracted by bulletin MS09-008, or more precisely, its part about WPAD. The bulletin fixes a number of vulnerabilities in Microsoft DNS and WINS services, including «WPAD Registration Vulnerability», but WPAD appears in security bulletin not for the first time. WPAD weaknesses were announced firstly in 1999, a wide range of problems closely associated with WPAD technology was published in 2007. In the same year Chris Paget showed WPAD vulnerabilities exploits at ShmooCon 2007. Now, 10 year later, Microsoft is publishing patches to fix WPAD flaws, but the question about security in networks, where WPAD is used, is still open. Successful attack on WPAD guarantees attackers full access on user data sent to Internet which could allow stealing critical data like passwords or credit card numbers. WPAD potential danger depends on two factors: default configuration and weak awareness among users.

In this article we discuss WPAD architecture and its many functioning principles in home and corporate networks, real examples of attacks and give recommendations for ordinary users and system administrators that allow reducing attack consequences.

2 WPAD review

WPAD (Web Proxy Auto Discovery) is a method used by web clients to automatically locate a browser configuration file used to connect through proxy. Microsoft proposed this protocol as a standard to IETF in 1999, but it was not approved. Now WPAD is supported by browsers Internet Explorer and Mozilla Firefox (Google Chrome and Apple Safari use Internet Explorer proxy configurations so they support WPAD too). WPAD is also supported by a number of operating systems, for example, by Konquerror browser in Linux.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

☐ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

☐ Bypass proxy server for local addresses

How to enable WPAD in Microsoft Internet Explorer

WPAD is a protocol used to locate a specific file (script) in a network. Methods and protocols used for searching are listed in WPAD specification. It is necessary to know automatic browser configuration scripts thoroughly to understand WPAD technology.

2.1 Proxy Auto Configuration scripts

File Proxy Auto Configuration (PAC file) is used in corporate networks to distribute browser configurations for proxy from a single source. Pracrically PAC is a script in JavaScript language which defines function FindProxyForURL(url, host):
url – запрашиваемый адрес;
host – is a part of url in «host name:port» format.

Example of PAC file:

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

This configuration file instructs the browser to use proxy server proxy.example.com for all web sites. Detailed description of PAC file syntax could be found in [3].

PAC files may be used with WPAD or separately, in this case you should explicitly specify the network path to the file in Internet browser settings.

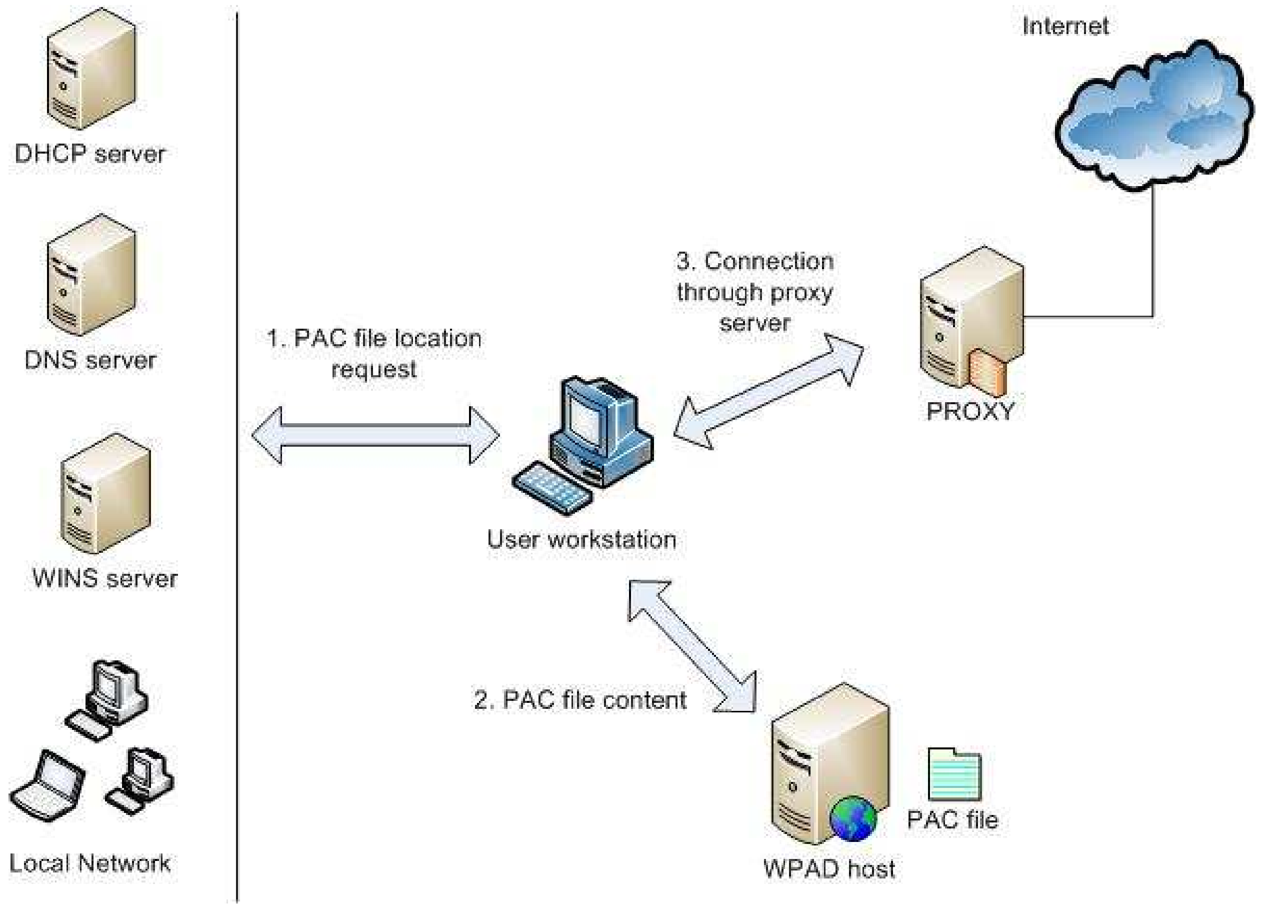
WPAD allows users to obtain PAC file location with one of the following methods:

- from DHCP server;
- request to DNS server;
- request to WINS server;
- NetBIOS Name broadcast request;
- hosts local file;
- lmhosts local file.

There are the following PAC file requirements if WPAD is used:

- PAC file should be located in root folder on web server;
- PAC flie name should be wpad.dat.

2.2 WPAD in corporate network



WPAD functioning principles

- Administrator creates a special configuration file (PAC file);
- Administrator reserves WPAD name for network host with Web server available on port 80/tcp. PAC file with wpad.dat name is located in the web server root folder;
- Client browser receives PAC file location;
- Browser reads the file via HTTP request;
- Browser configures proxy server settings.

3 Web Proxy Auto Discovery attack scenarios

WPAD is enabled by default in Internet Explorer which makes computers of a great number of the browser's users vulnerable. Computers with browsers that import Internet Explorer settings are also vulnerable. According to SpyLog data in April 2009 Internet Explorer, Apple Safari and Google Chrome are used by 55% of Russian segment of users.

The most vulnerable part in WPAD technology is PAC file location search. If an attacker persuades the user that configuration file on attacker's host is a required file then the attack seems to be successful.

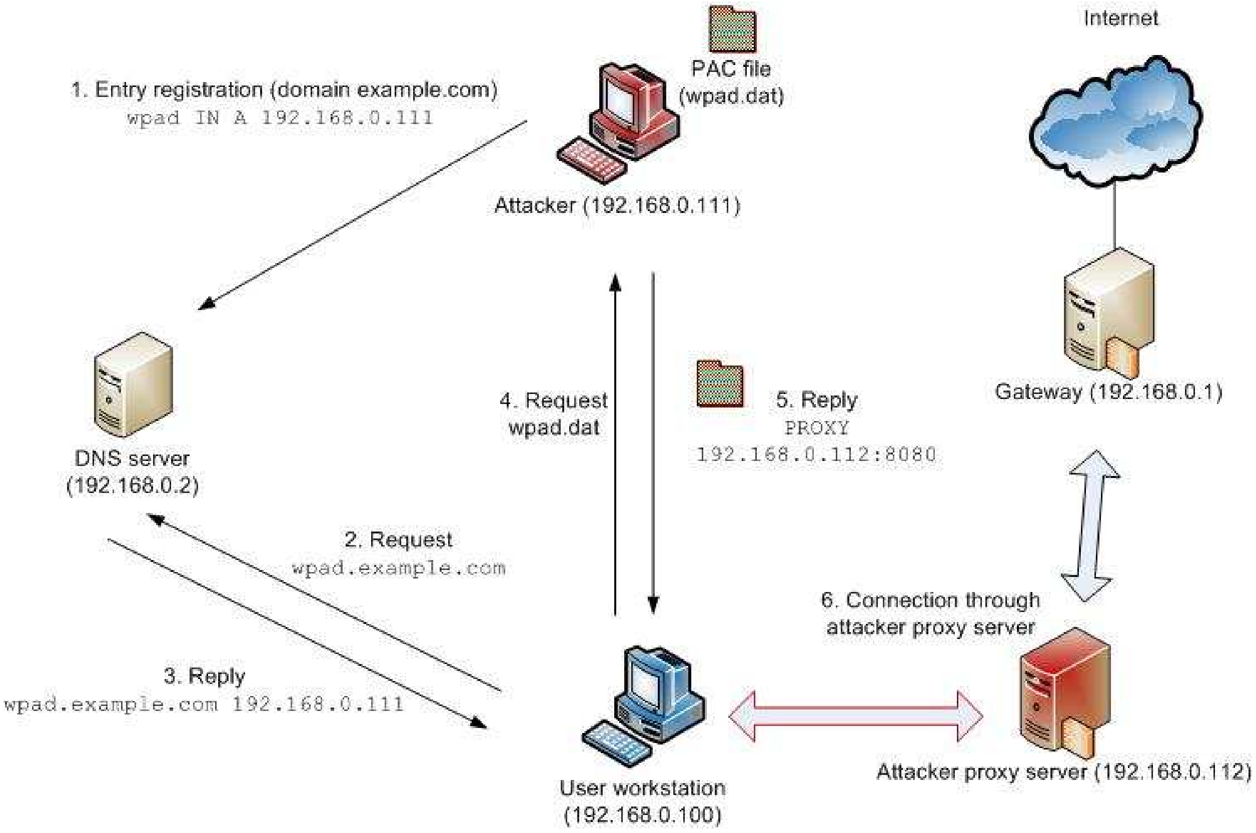
To conduct the attack successfully an attacker should have:

1. Web server to locate specially crafted PAC file on it;
2. Proxy server controlled be the attacker;
3. Tools to control traffic according to objectives: SSL session hijacker, network packet analyzer, etc.

Attacks based on malicious DHCP server injection is beyond the scope of the article as this attack allows to fully control all client network subsystem settings, as well as WPAD. Further we assume that PAC file location is not distributed via DHCP. We will take that hosts and lmhosts local files are unavailable for attackers.

3.1 Attacks based on DNS server usage

DNS system supports record dynamic updates that allow clients to register their names and IP addresses on DNS server automatically when they log on into the network or change IP addresses via DHCP server. If unauthenticated dynamic updates are allowed in attacked zone than one special DNS packet is enough to register a record.



Attack scenario with DNS server usage

On the picture above you can see a general scheme of an attack. Attacker proxy server and PAC file distribution point could be located on the same network host.

1) Attacker register the following record on DNS server:

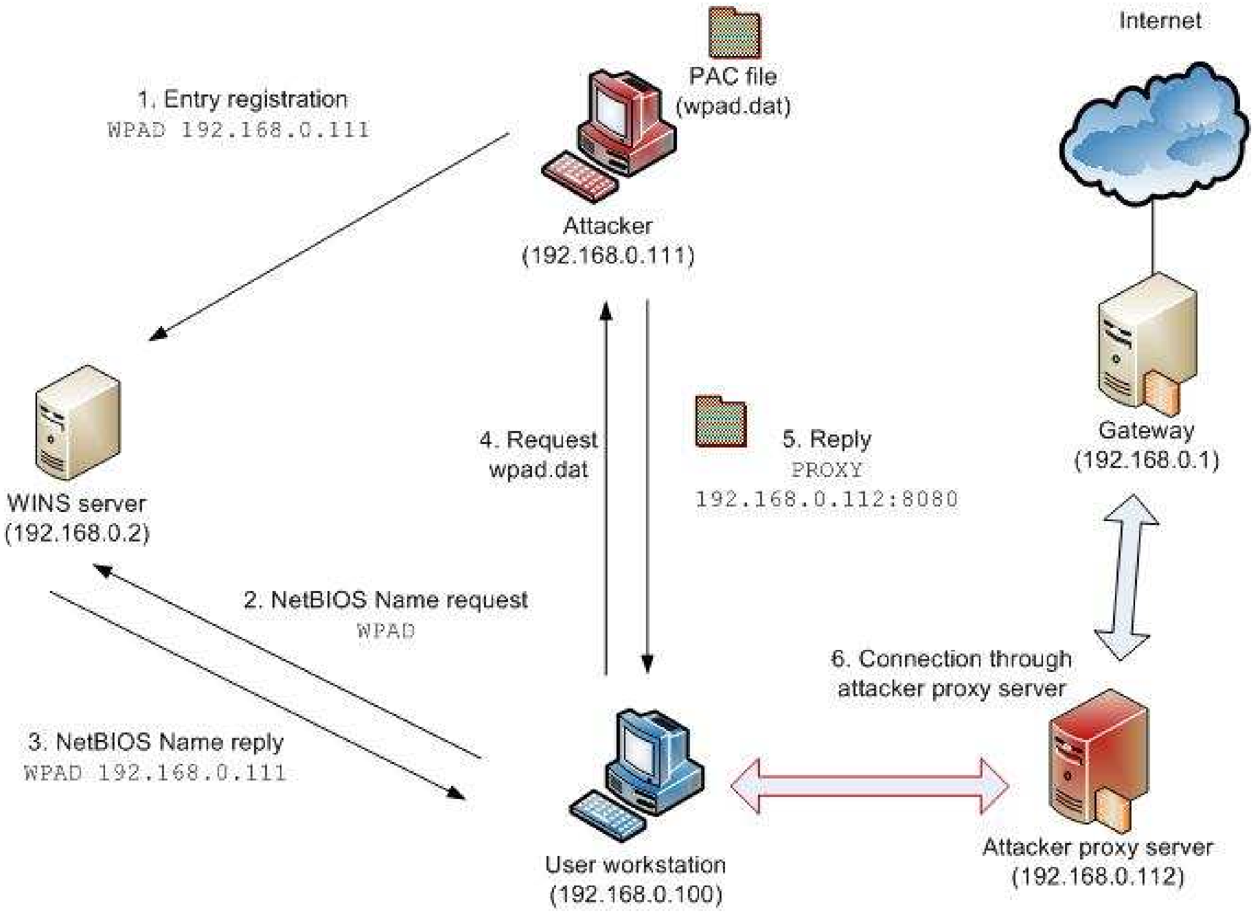
   wpad.<attacked domain> IN A <attacker IP address>.
2) Client requests wpad.<domain>host IP address from DNS server;
3) DNS server returns attacker IP address;
4) Client requests PAC file (wpad.dat);
5) Client configures a browser according to PAC file;
6) All client traffic goes through attacker proxy server.

Notes: If DNS server works in Active Directory then more secure configuration is possible that allows record dynamic updates for authenticated users only. It this case an attacker should have valid account in attacked domain to conduct a successful attack. [4]

This class of attack is actual only for network with domain structure, as PAC file location request to DNS server is not used in networks based on working groups. Both domain and non-domain networks are vulnerable to attacks described below.

3.2 Attacks based on WINS server usage

Network computer name registration is WINS server normal function. Similar to DNS server the registration is done via one special packet.



Attack scenario with WINS server usage

1) Attacker register the following record on WINS server:

   WPAD <attacker IP address > (Unique record type)

2) Client requests IP address of a host with WPAD NetBIOS name from WINS server;

3) WINS server returns attacker IP address;

4) Client requests PAC file (wpad.dat);

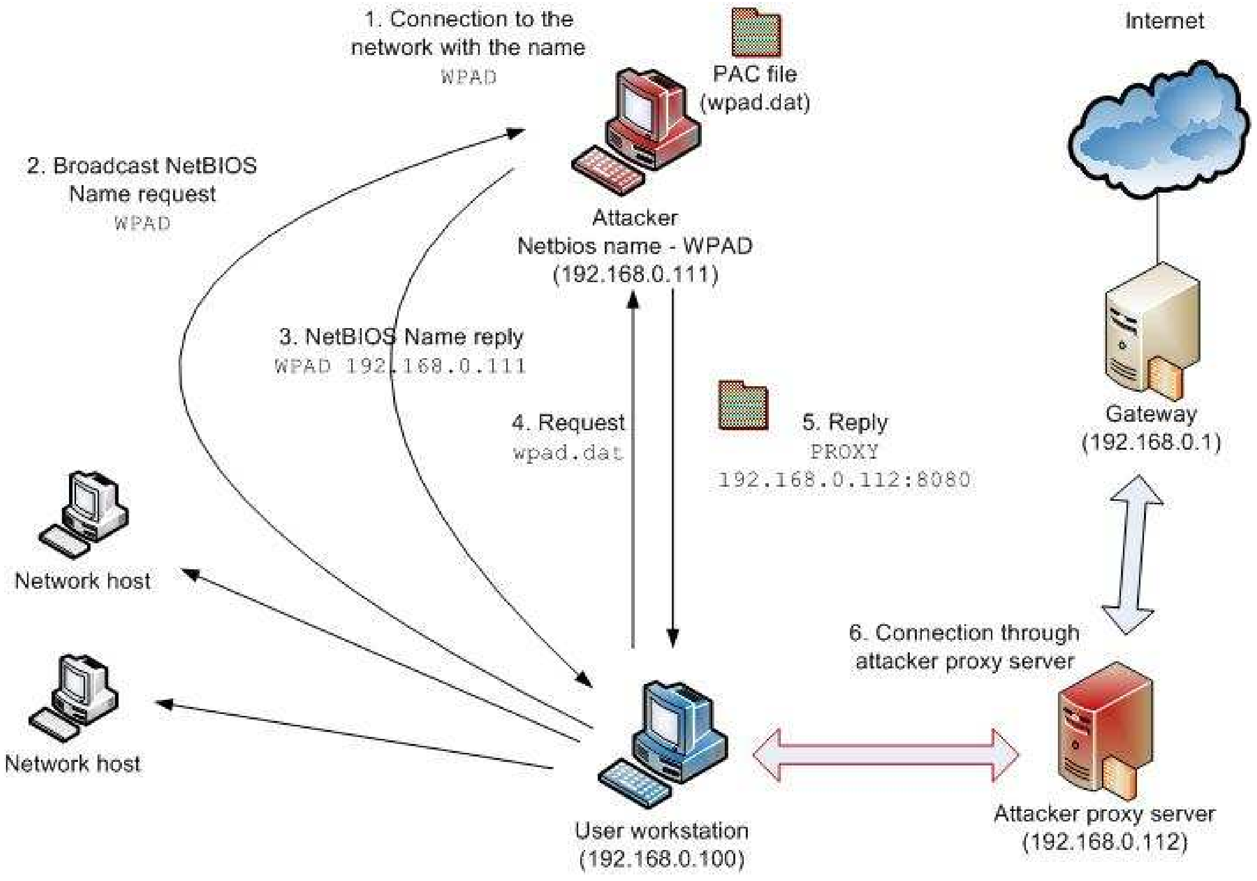
5) Client configures a browser according to PAC file;

6) All client traffic goes through attacker proxy server.

3.3 Attack in available sub network

If DNS and WINS servers are not able to locate PAC file then according to WPAD standard web clients make broadcast NetBIOS WPAD name request to sub network clients following network mask.

His attack vector is available only if an attacker has physical access to client sub network.



Attack scenario in available sub network

1) Attacker log on into the network with WPAD NetBIOS name;

2) Client requests WPAD name in broadcast request;

3) Attacker replies with his IP address;
4) Client requests PAC file (wpad.dat);
5) Client configures a browser according to PAC file;
6) All client traffic goes through attacker proxy server.

The class of attacks described above is easily implemented in most part of networks without strict security policy, as an example, in home networks, networks of small Internet provider companies, WiFi in cafes and shopping malls, where WINS servers are not used, and NetBIOS traffic is not filtered on network devices.

4 WPAD in Microsoft services

WPAD is used to find proxy server in a number of Microsoft system components besides browsers:

- Windows Update service. This service uses WPAD to look for Microsoft updates distribution point;
- Microsoft Crypto API. Crypto API uses WPAD for updating CRL (Certificate revocation list) or Root CA (Root Certificate Authority);

These services always use WPAD regardless of Internet Explorer settings.

Note: Windows Update and Crypto API send only signed data so they are not vulnerable to «man-in-the-middle» attack. Above attacks can cause incorrect functioning of these services.

- Microsoft Firewall client for ISA server. With certain settings this application searches for ISA server vie WPAD request to DNS server.

5 How to fix WPAD Registration Vulnerability

The following vulnerabilities are fixed in the bulletin MS09-008:

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

In spite of the vulnerability name, updates installation does not make any changes to the name registration process, some adjustments are made only into DNS-and NetBIOS-name resolving process. Before looking into database, DNS and WINS servers are trying to find requested name in blacklist. If the name is in blacklist then the client receives error code "name is not found". Otherwise server continues normal work.

Blacklists only reduce the potential scale of the attack - possibility to use own DNS and WINS server entries for attackers, but available subnet attack is also possible to conduct. Microsoft experts explain such behavior with concern for customers that have deployed and now actively use WPAD technology.

Blacklists are stored in the following register keys:

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

Default blacklist elements:
«wpad isatap» for DNS server;
«WPAD WPAD. ISATAP» for WINS server.

Please note that if at the time you install the update some of above entries exists in WINS or DNS database, they are not added to the list.

Blacklists are used only for dynamic entries, so administrators could organize a network with WPAD registering static entries in DNS and WINS databases.

Note: dynamic entries are added to DNS and WINS server databases with special registration request, static entries are added through server console.

Let's look in detail on the names added to blacklists. This article covers WPAD names. WPAD. (WPAD with dot) is used in Windows Updates and Crypto API components, ISATAP is required to find routers supported ISATAP protocol. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an IPv6 transition mechanism meant to transmit IPv6 packets on top of an IPv4 network. ISATAP name attacks are not described in the article as Ipv6 is not popular and is used rarely.

6 Recommendations how to fix the vulnerability

6.1 For end users

- Disable WPAD support in browser settings;
- Specify PAC file distribution point in browser settings if in your network proxy server is configured via PAC file, and its location is known in advance.

6.2 For system administrators

Due to vulnerability specific characters networks which do not use Web Proxy Auto Discovery are more vulnerable then networks with configured WPAD. The following actions will help to strengthen security protection:

- Disable WPAD support;
- Reserve WPAD and WPAD. Names via DNS and WINS static entries, for example for IP address 0.0.0.0. Microsoft WINS server does not allow registering names for invalid IP addresses but Chris Paget shows a method how to bypass this restriction: it is possible to reserve a name for valid IP address and then change it to IP address 0.0.0.0.

There are additional methods to strict security level in Active Directory domian:

- Allow only authenticated updates of entries on DNS server;
- Distribute PAC file location via group policy.

7 Conclusions

The main reason that makes attacks via WPAD such dangerous is that it is widely used in default configuration. Now Microsoft is actively promoting the approach Secure by Default as one of the fundamental principles of SDL (Security Development Lifecycle) but proxy server configuration in Internet Explorer is a vivid example of the violation of this principle.

WPAD weaknesses are widely known from 1999, but it is still used. There is a great deal of Microsoft dominance in Internet browser market, and even the fact the there is no WPAD standard could not stop the spread of this technology.

This article describes only simple attacks via WPAD, but there are more complicated attacks which require additional methods to bypass security protection system. IP address spoofing in registration packets or corporate DNS server temporary outage could help to bypass several restrictions on vulnerability exploitation. When choosing protection mechanisms, network administrators should take into account a wide range of possible attack vectors, as well as the fact that the Microsoft updates fix the vulnerabilities only partly.

As WPAD vulnerabilities are not eliminated yet, attackers have a wide range of possible attacks to conduct.

It is possible that while you are reading this article, your browser is looking for a magic WPAD name☺

8 About Me

Graduated from Moscow State Technical University named after Bauman. Now I am an expert in cryptography and secure data exchange protocols. I specialize in analysis of network service vulnerabilities and design extensions for Positive Technologies MaxPatrol network scanner.

9 About Positive Technologies

Positive Technologies www.ptsecurity.com is among the key players in the IT security market in Russia.

The principal activities of the company include the development of integrated tools for information security monitoring (MaxPatrol); providing IT security consulting services and technical support; the development of the Securitylab en.securitylab.ru leading Russian information security portal.

Among the clients of Positive Technologies there are more than 40 state enterprises, more than 50 banks and financial organizations, 20 telecommunication companies, more than 40 plant facilities, as well as IT, service and retail companies from Russia, CIS countries, Baltic States, China, Ecuador, Germany, Great Britain, Holland, Iran, Israel, Japan, Mexico, South African Republic, Thailand, Turkey and USA.

Positive Technologies is a team of highly skilled developers, advisers and experts with years of vast hands-on experience. The company specialists possess professional titles and certificates; they are the members of various international societies and are actively involved in the IT security field development.

10 Links

1. Chris Paget report at ShmooCon 2007
   http://video.google.com/videoplay?docid=-4596414840866123044
2. WPAD in Wikipedia
   http://en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol
3. PAC file examples
   http://www.findproxyforurl.com/
4. DNS dynamic updates in Windows 2003 Server
   http://support.microsoft.com/kb/816592
5. Name resolving
   http://www.comptechdoc.org/os/windows/wintcp/wtcpname.htmll
6. Changes to WINS server behavior after you install the security update for WINS server
   http://support.microsoft.com/kb/968731
7. ISATAP in Wikipedia
   http://en.wikipedia.org/wiki/ISATAP
8. DNS security protection for Windows
   http://www.windowsecurity.com/articles/Securing_windows_2000_DNS_by_using_configuration_Part_2.html
9. Web Proxy Auto-Discovery Vulnerability (Microsoft Security Advisory)
   http://www.microsoft.com/technet/security/advisory/945713.mspx
10. WPAD Spoofing Vulnerability (Microsoft Security Bulletin)
    http://www.microsoft.com/technet/security/bulletin/ms99-054.mspx
11. WPAD Registration Vulnerability (Microsoft Security Bulletin)
    http://www.microsoft.com/technet/security/Bulletin/MS09-008.mspx
12. The utility designed by Positive Technologies to detect potentially dangerous entries in DNS and WINS name servers.
    http://www.securitylab.ru/news/extra/380522.php
13. WPAD standard draft
    http://www.cam.ac.uk/cs/webcache/draft-cooper-webi-wpad-00.txt