# POSTER: Sniffing and Propagating Malwares through WPAD Deception in LANs

Li Dan[1,2], Liu Chaoge[2], Cui Xu[3], Cui Xiang[2]
[1]Beijing University of Posts and Telecommunications
[2]Institute of Computing Technology, Chinese Academy of Sciences
[3]China Academy of Aerospace Aerodynamics
lidan@software.ict.ac.cn

## ABSTRACT
The Web Proxy Auto-Discovery (WPAD) protocol is always used to locate a URL of a configuration file through DHCP, DNS or some other discovery methods. WPAD is a very convenience way for the management of network administrator. However, in the meantime, it may lead to a potential compromise to our LANs. In this poster, we propose a novel attack method based on WPAD protocol which can be used by attacker to intercept traffic, sniff and propagate malwares in LAN.

## Categories and Subject Descriptors
C.2.1 [**Computer Communication Networks**]: Network Architecture and Design

## General Terms
Design, Security

## Keywords
WPAD, Malware Propagation, Sniffer

## 1. INTRODUCTION
Nowadays, most browsers allow users to configure proxy servers. Mainly, there are three methods can be used: ***Manual Configuration*** in which users set the IP and Port of proxy manually, ***Proxy Auto-Config (PAC)*** in which users set a PAC file manually which includes the information of proxies and ***Web Proxy Auto-Discovery*** in which browsers can automatically discover the PAC file by WPAD protocol without manual configuration (e.g., Internet Explorer provides those three methods that can be found in the option "Tools->Internet Options ->LAN Settings").

WPAD protocol is always used by clients to locate a URL of a configuration file. It is designed to simplify settings, facilitate deployments in large-scale networks. However, this mechanism will also bring security threats (e.g., the famous malware "Flame" which uses windows update as one of its methods to propagate malware is based on this mechanism). An attacker can use this mechanism to hijack users' browser, especially in some public areas (e.g., airports, cafe).


*CCS'13,* November 4–8, 2013, Berlin, Germany.
ACM 978-1-4503-2477-9/13/11.
http://dx.doi.org/10.1145/2508859.2512520

## 2. MECHANISM OF WPAD
### 2.1 Definitions
**WPAD client:** WPAD client is a host which opens Web Proxy Auto-Discovery and queries for proxy's information in LAN.

**WPAD server:** WPAD server is a host which provides proxy's information and responds requests from WPAD clients.

### 2.2 Working Processes
WPAD clients have six approaches to search WPAD servers in windows operating system: query through DHCP (option 252) protocol, query through DNS protocol, query through WINS protocol (host name is "wpad"), query through NetBIOS broadcast, query through "hosts" file and query through "lmhosts" file. WPAD clients will query through those methods one by one in a specific order until an available WPAD server is found. All the six methods can be used to redirect browser's traffic and the first four methods can be used through networks.

After a WPAD server is found in the LAN, a browser configured to use Web Proxy Auto-Discovery mechanism will automatically download a PAC file. The PAC file includes a function named "FindProxyForURL(url, host)" which is written in javascript. This function is called by the browser of WPAD client for each URL request. When this function is called, the IP address and port to be accessed from the original URL is ignored and the "host" parameter of the function returns the real IP and port for this request.

## 3. DECEPTION OF WPAD CLIENTS
There is an illustration of WPAD deception through NetBIOS broadcast. We assume that an attacker can interconnect to a LAN as a normal user in it (may through physical access or control a user's computer in the LAN). With the ability to interconnect with all the users in the LAN, the attacker can imitate the WPAD server to respond WPAD Clients' NetBIOS broadcast queries. For windows operating system has the mechanism to avoid the conflict of more than one WPAD server in LAN, an attacker can easily imitate and kick off the real WPAD server. The process of WPAD deception through NetBIOS broadcast is illustrated in Figure 1 and 2.

1. **Query the WPAD server in LAN:** When the browser of a WPAD client is opened for the first the time, it will query the WPAD server automatically.
2. **Respond as a WPAD server:** the attacker monitors UDP broadcasts packets of NBNS protocol at port 137. If a NBNS name query request is found, the attacker will respond those queries to claim that it is a WPAD server.

3. **Request the PAC file:** When the client receives the response from the attacker, it will consider the attacker as the WPAD server and the client's browser will request the PAC file named "wpad.dat" from it.

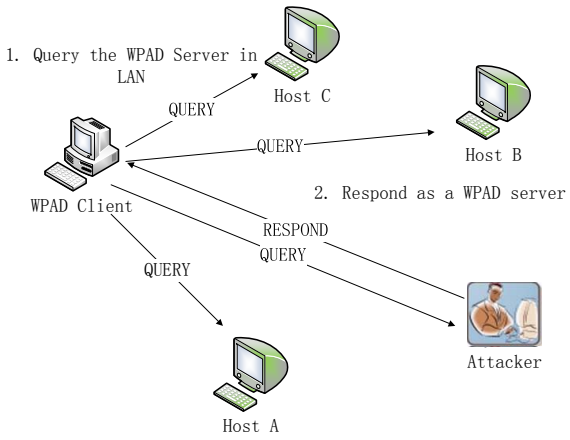


**Figure 1. The attacker claim itself a WPAD server.**

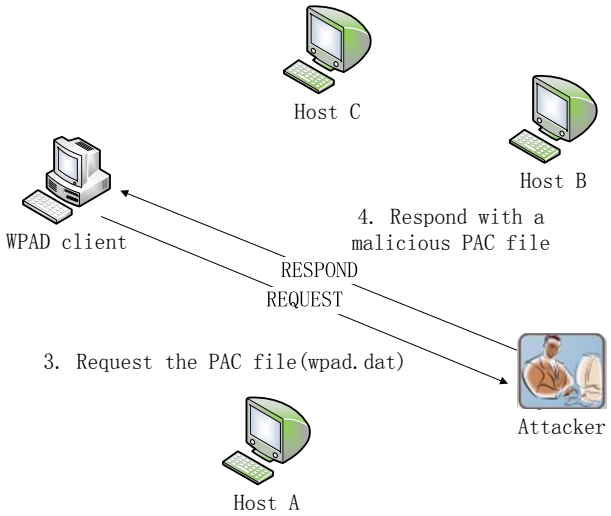


**Figure2. The WPAD client downloads the PAC file.**

4. **Respond with a malicious PAC file:** the attacker waits for clients' request of PAC file and respond with a malicious one including the "FindProxyForURL" function.

# 4. SNIFFING AND PROPAGATING MALWARES IN LAN

When the client's browser get the PAC file successfully, it will call the "FindProxyForURL" function for each URL requested from the client and send the client's request to the host returned from this function (not all the browsers call this function when Web Proxy Auto-Discovery mechanism is opened, we know Internet Explorer under version 9, most version of firefox and safari will do that as so far).

An attacker can use the "FindProxyForURL" function to redirect all victims' browser's traffic to a specific proxy server set up beforehand to ***sniffing all the traffic in LAN.*** Meanwhile, the proxy server can detect the URL to be accessed by users. If the URL requests to download a file (e.g., URL ended with "rar", "exe", "doc", "pdf", etc.), the attacker can replace the file and return a malicious one that has the same name with the original one to the user. It is hard for the user to find the downloaded file is changed and the malware will have a higher possibility to be run. If there is a host invaded by an attacker, it can use that method to ***propagating malwares in LANs***.

# 5. PRELIMINARY RESULTS AND LIMITATIONS

## 5.1 Preliminary Results

We preliminary implement a prototype of WPAD deception implement base on NetBIOS broadcast. The experimental result is illustrated in Figure 3.

The "wpad.dat" file provided by "hfs.exe"(in the upper right) is downloaded multi-times.
The hosts in the LAN access the internet through a proxy server named "HttpProxyServer.exe" (In the lower right) and log the IP addreses at the same time.
Those packets captured by "Wireshark.exe"(in the left) shows the detail of WPAD deception.

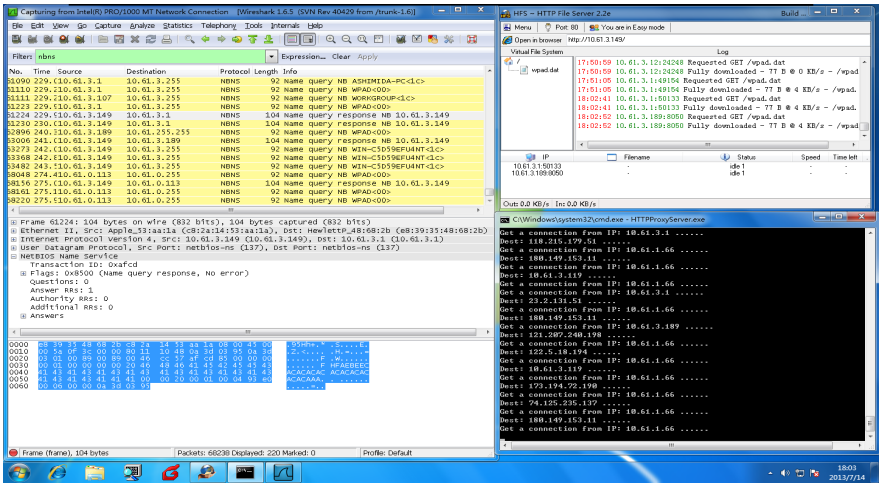

**Figure3: experimental result of WPAD deception**

**Table 1. Table captions should be placed above the table**

| Version of system | Version of Browser | Is "Automatic Detection Setting" be configured by default | Is WPAD deception succeed if "Automatic Detection Setting" is configured |
|---|---|---|---|
| Windows xp sp2 Home Edition | IE 8 | YES | YES |
| Windows xp sp3 Home Edition | IE 8 | YES | YES |
| Windows xp sp3 Professional | IE 8 | NO | YES |
| Windows 7 Home Basic | IE 8 | YES | YES |
| Windows 7 Home Basic | IE 9 | YES | NO |
| Windows 7 Ultimate | IE 8 | YES | YES |
| Windows 7 Ultimate | IE 9 | YES | NO |
| Windows 8 Ultimate | IE 10 | YES | NO |

## 5.2 Limitations

WPAD deception is largely depends on the implement of browsers. For example, in Internet Explorer, although the file "wpad.dat" is always been downloaded when "Automatic Detection Setting" is set, the "Internet Explorer" will not use the auto-detected proxy to access internet after version 9 in our experiment. The "Automatic Detection Setting" is also default configured only in part of versions of windows system. The default configurations and the experimental results from part of versions of Windows XP to Windows 7 is listed in table 1.

# 6. FUTURE WORKS

Table 1 shows that "Automatic Detection Setting" is configured by default in part of version of Windows xp, all versions of Windows 7 and in Windows 8. But WPAD deception only succeed before IE 9. For WPAD is a convenient method for intranet management, it should be supported in IE 9 and versions above. In the future, we will try to find whether there are some mechanisms we don't notice and other three query methods that can be used in LAN.

# 7. ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under grant (No. 61202409) and the National High Technology Research and Development Program (863 Program) of China under grant (No. 2012AA012902 and 2011AA01A103).

# 8. REFERENCES

[1] WPAD: Internet Explorers Worst Feature, Grant Bugher, <http://perimetergrid.com/wp/2008/01/11/wpad-internet-explorers-worst-feature/>

[2] HTTP: The Definitive Guide, David Gourley, Brain Totty