

# Getting rid of WPAD vulnerability – From Registry's Perspective –

February 25, 2008

APTLD in Taipei

Yoshiro YONEYA, JPRS

<yone@jprs.co.jp>

<http://日本レジストリサービス.jp/>

## Contents

- What happened?
- Reaction of Registries
- What is 'WPAD vulnerability'?
- Why WPAD introduces vulnerability?
- What JPRS did against WPAD vulnerability

# Microsoft Security Advisory (945713)

<<http://www.microsoft.com/technet/security/advisory/945713.msp>>

The screenshot shows the Microsoft TechNet website interface. At the top, there is a navigation bar with "United States Change" and "All Microsoft Sites". Below this is the "Microsoft TechNet" logo and a search bar for "Search Microsoft.com for:". A secondary search bar is located on the left side of the page. The main content area displays the title "Microsoft Security Advisory (945713)" and the subtitle "Vulnerability in Web Proxy Auto-Discovery (WPAD) Could Allow Information Disclosure". The advisory is dated "Published: December 3, 2007 | Updated: January 9, 2008". The text describes a vulnerability in the way Windows resolves hostnames that do not include a fully-qualified domain name (FQDN). It states that Microsoft is aggressively investigating the public reports and that customers whose domain name begins in a third-level or deeper domain, such as "contoso.co.us", are at risk from this vulnerability. The advisory concludes by stating that upon completion of the investigation, Microsoft will take appropriate action to help protect customers, which may include providing a security update through the monthly release process or an out-of-cycle security update, depending on customer needs.

## What happened?

3 Dec 2007: Advisory published (by Microsoft)

4 Dec 2007: Issues discussed among registries

---

JPRS

6 Dec 2007: temporarily blocked the registration of  
'WPAD' as the 3rd and further level domain labels

12 Dec 2007: decided the label 'WPAD' to be reserved

14 Dec 2007: announced its action to registrars,  
CERT, and ISP associations

19 Dec 2007: announced its action to hosting providers

21 Dec 2007: announced its action to the public

# Reaction of Registries

acknowledged by JPRS  
as of December, 2007

TLD	Block of wpad.**.tld	Remarks	Info source	Date
.fr	Y		C	5 Dec 07
.pl	N	Already registered	C	5 Dec 07
.at	N	Already registered	C	5 Dec 07
.au	Y		A	6 Dec 07
.lt	Y		C	6 Dec 07
.jp	Y		A/C	6 Dec 07
.mn	Y		A	21 Dec 07

Y:Yes  
N:No

A:member@aptld  
C:tech@centr

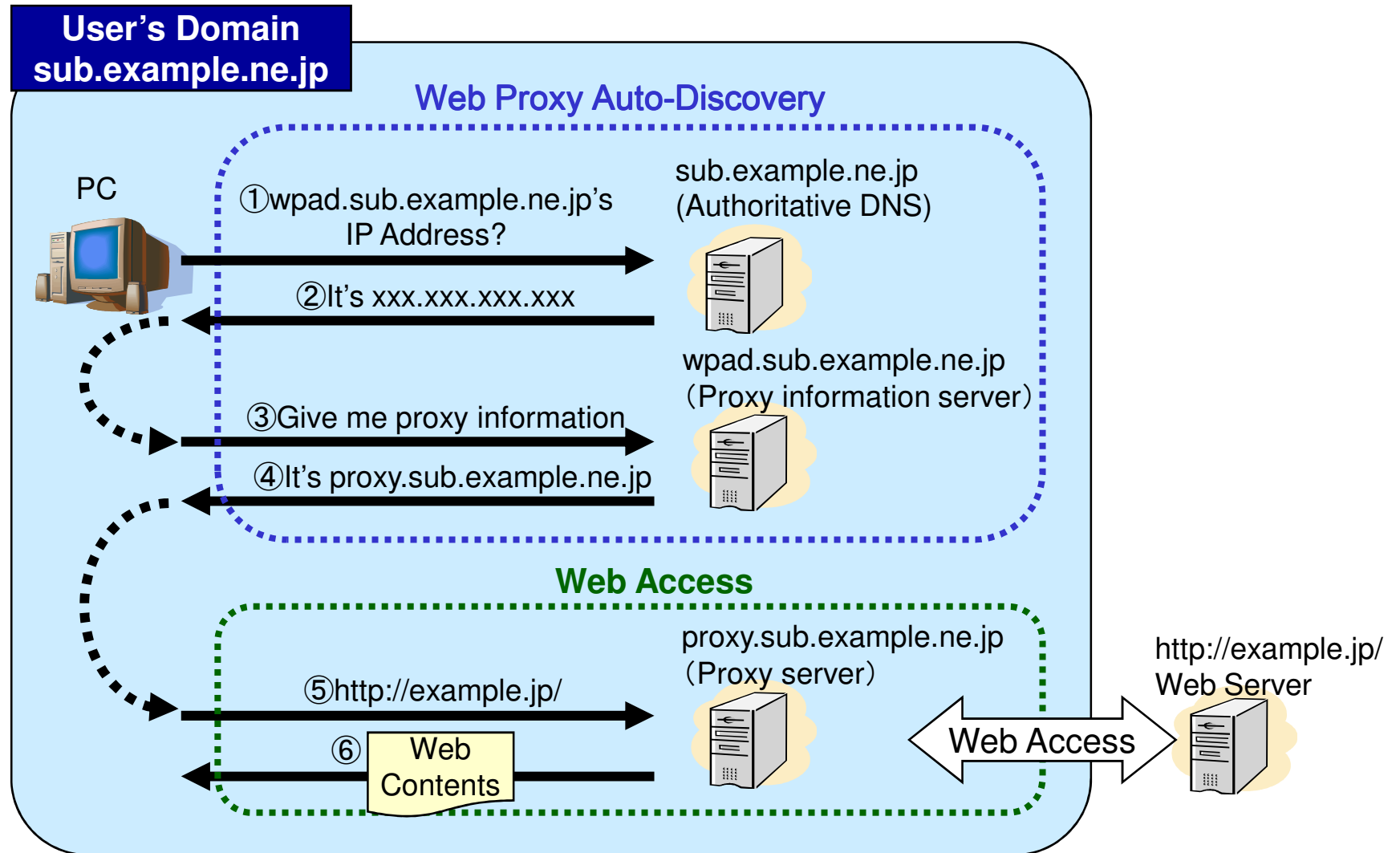
## What is 'WPAD vulnerability'?

- In some circumstances, 3rd party can steal victims' web accesses
- Conditions are:
  - Victim's PC is configured to use Web Proxy Auto-Discovery (WPAD)
  - Victim's PC is configured to use Domain Suffix
  - No appropriate WPAD server is provided in victim's organization
  - Domain name of victim's organization is registered as 3LD or further
  - 3rd party has domain name 'WPAD' under the same 2LD

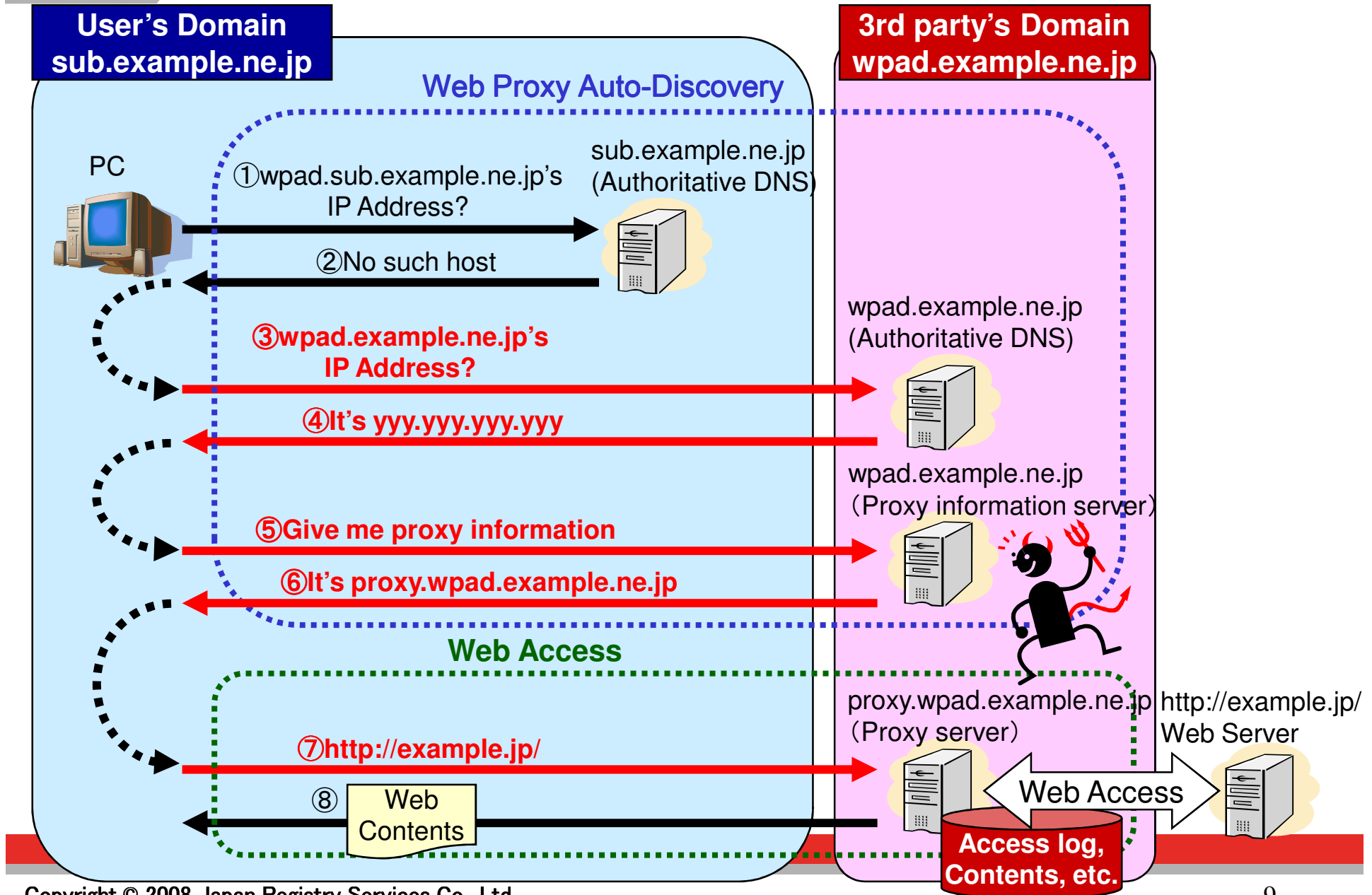
## Why WPAD introduces vulnerability?

- WPAD protocol is 'de facto' protocol
    - No standard (RFC)
    - Assumes literal name 'WPAD' as a proxy information server
    - Behavior is implementation dependent
    - Vulnerability was found in Microsoft's implementation  
<<http://www.microsoft.com/technet/security/advisory/945713.msp>>
  - Microsoft's implementation
    - Tries to resolve the name 'WPAD' down to 3LD by eliminating the domain label following 'WPAD'
- (1) `wpad.sub.example.ne.jp` } failed  
 (2)     `wpad.example.ne.jp` } failed  
 (3)             `wpad.ne.jp` } failed
- } *registrants may differ!*

Normal case: Expected behavior of WPAD



Vulnerable case: Victim's PC uses 3rd party's web proxy server



## What JPRS did against this vulnerability

Step0: Made the label 'WPAD' reserved under 3LD

Step1: Announced it to registrars first

- Not to affect their hosting services

Step2: Contacted to CERT organizations / ISP associations just after the step1

- To obtain wider reachability for hosting providers

Step3: Announced it to hosting providers

- Not to affect their hosting services

Step4: Announced it to public

**➔ No claim / objection raised from community**