https://www.us-cert.gov/ncas/alerts/TA16-144A

Alert (TA16-144A)
WPAD Name Collision Vulnerability

New attack vector based on combination of
CVE-2007-5355, CVE-2009-0093, and CVE-2012-4776

Systems Affected:

Windows, OS X, Linux systems, and web browsers with WPAD enabled

Patrik Fältström - paf@netnod.se
Chair SSAC

Background

- Web Proxy Auto-Discovery (WPAD) Domain Name System (DNS) queries that are intended for resolution on private or enterprise DNS servers have been observed reaching public DNS servers.

- Leaked WPAD queries could result in domain name collisions with internal network naming schemes.

- Collisions could be abused by opportunistic domain registrants to configure an external proxy for network traffic, allowing the potential for man-in-the-middle (MitM) attacks across the Internet.

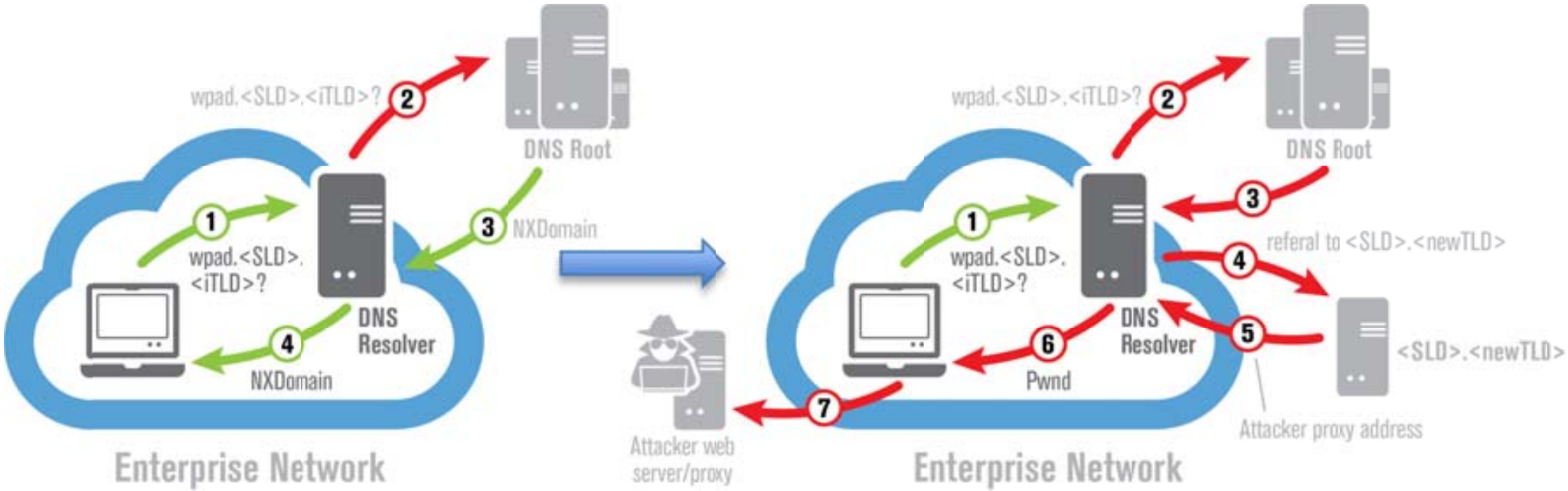

Figure 1 This Figure illustrates how queries for iTLDs can get leaked to the global DNS root, and then used by an attacker to launch a MitM attack, either via the same server, or a server located anywhere else on the Internet.

Supported OSes and browsers		Verified versions for DNS WPAD	Enabled by default
Browser	Internet Explorer	6–11	Yes
	Chrome	43	No
	Firefox	12, 33	No
	Safari	8	No
OS	Windows OS	XP, Vista, 7, 8, 8.1, 10	Yes
	Ubuntu	12.04, 14.04	No
	Mac OS X	10.10	No

What we know:

- Given use of **example** as internal TLD, **wpad.example** is looked up, and **wpad.dat** is fetched.
- Given popular internal TLDs are to be delegated, **.corp**, **.dev**, **.network**, we increase the risk for name collisions, for certificates and more.
- SSAC, Verisign, and others forewarned about this 3+ years ago (so the technology and ideas used are not new).

1. Yeti DNS Project https://yeti-dns.org/

What we did not know

- Not only Microsoft platforms are vulnerable, the wpad issues affect **any** system where it is configured.
- If an enterprise uses an iTLD as its AD Domain name (such as **.corp**), and doesn't respond to DNS queries for that domain, then queries like **wpad.*something*.corp** are sent outside the enterprise to the public DNS root.
- About 20 million vulnerable queries are visible every day. Attackers can remain off-path, always-on and just wait to get a query.
- The difference between before and now is that SLDs within new gTLDs that can enable exploitation **are** being registered, and there are still millions of devices at risk, moreso now than ever!
- Let's then add dotless domains, wildcard, democratized root[1] (absent DNSSEC validation)… and you get the full picture. Specifically dangerous is this for corporate devices that are used outside of the corporate network.

1. Yeti DNS Project https://yeti-dns.org/

What to do?

- Disable automatic proxy discovery/configuration in browsers and operating systems.
- Use a fully qualified domain name (FQDN) from global DNS as the root for enterprise and other internal namespace.
- Configure internal DNS servers to respond authoritatively to internal TLD queries.
- Configure firewalls and proxies to log and block outbound requests for wpad.dat files.
- Identify expected WPAD network traffic and monitor the public namespace or consider registering domains defensively to avoid future name collisions.
- File a report with ICANN if your system is suffering demonstrably severe harm as a consequence of name collision by visiting https://forms.icann.org/en/help/name-collision/report-problems.

Thanks!

- **MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era**
  Qi Alfred Chen, Z. Morley - University of Michigan
  Eric Osterweil, Matthew Thomas - Verisign Labs

- Danny McPherson - Verisign
  Warren Kumari - Google
  Other SSAC members

http://shorl.com/stuhiprudryvidri