

DNS attacks

The Domain Name System (DNS) is used to map names to IP addresses. Modern DNS implementations are secure against a number of protocol-based attacks. However, many systems are still vulnerable to policy-based attacks.

DNS Servers have traditionally offered simple name to address mappings. More complex behavior such as filtering of packet contents has been poorly deployed. These limitations can be used by attackers to convince end hosts to engage in inappropriate behavior.^{1 2}

> DNS Rebinding

An attacker can use your "private" IP addresses in his "public" DNS zone. When an employee visits the attackers web site, the javascript can access hostnames within the attackers zone. These names resolve to your "private" addresses, which is a clear violation of security policy. The attacker can then scan your entire network via a malicious javascript application. The solution is to filter out "your" addresses when they appear inside of an attackers DNS records.

> Public DNS Rebinding

This attack is the same as above, except that the attacker puts one of your "public" IP address into his zone.³ The same javascript as above can be used to access any service hosted at that address. Since the access is made from a private address "inside" of your company, many security restrictions can be bypassed. The solution is to filter out "your" addresses when they appear inside of an attackers DNS records.

> Leaking Private Addresses

An attacker can query your public DNS zone information, and often find records containing private IP addresses.⁴ This gives the attacker information about the internal structure of your company, including which applications are used, and which targets to attack. The solution is to ensure that private addresses are never exposed in a public zone. Many DNS servers do not even filter private addresses from public zones.

> Summary

Most DNS deployments are vulnerable to the attacks outlined here. Some DNS vendors have products which may not be vulnerable to these attacks when configured correctly, but which are usually misconfigured in practice. In the end, the result is the same: your business is vulnerable to attacks which have been known and resolved for years.

These attacks all have a common element: they leverage the differences between DNS and network configurations. The Mancala Network Controller automatically monitors network configuration and updates DNS behavior to ensure real-time synchronization and security.

¹ <http://www.kb.cert.org/vuls/id/800113>

² <http://www.cert.org/advisories/CA-2002-19.html>

³ <http://blogs.techrepublic.com/security/?p=4197>

⁴ <http://blog.sucuri.net/2010/05/leaking-private-ip-addresses-via-dns.html>