(UPDATED) AUGUST 2012

Domain Name System: Security strategies

1. This report provides information on Domain Name Service (DNS) security, for Australian Government users. Misconfigured DNS systems, known as resolvers, are vulnerable to a number of security exploits which could lead to data compromises. The report provides information on protecting DNS integrity and provides strategies to reduce the likelihood of DNS resolver compromise.

2. CSOC recommends that agencies implement the recommendations in this document as a priority. Following the recommendations in the report will help to ensure that through correct DNS system configuration and management, users are directed to genuine rather than malicious websites.

3. DNS is a hierarchical naming system built on a distributed database for resources connected to the internet. DNS maps domain names to their corresponding IP addresses and vice versa.

For example, www.agency.gov.au ⟷ 192.0.32.10

Background

4. DNS has no authentication mechanisms included by default. The lack of authentication increases the risk of falsified DNS information being stored on your agency's DNS resolver by hosts with no authority to do so. These activities are known as DNS spoofing and DNS cache poisoning.

5. DNS spoofing and cache poisoning can permit an cyber actor to map the internal network of your agency based on queries from the internal DNS resolver to upstream DNS resolvers. DNS cache poisoning can subvert client connections to provide false information, facilitating installation of malicious code or the extraction of sensitive information.

6. DNS resolvers are typically configured to query upstream counterparts if they do not have an entry cached for the requested domain name. This is known as recursion, or caching. Recursion improves response times and performance by caching replies similar to the way in which history is cached by a web browser. Entries will remain in a DNS resolver's cache depending on the time to live (TTL) value in the returned record. A common TTL value for DNS is 86400 seconds (24 hours).

7. Configuring a recursive DNS resolver on your network to allow external access permits parties to masquerade as your agency when performing DNS queries – perhaps to inappropriate sites.

Normal DNS resolution

8. During the normal DNS resolution process, clients are provided with correct IP addresses for requested sites:

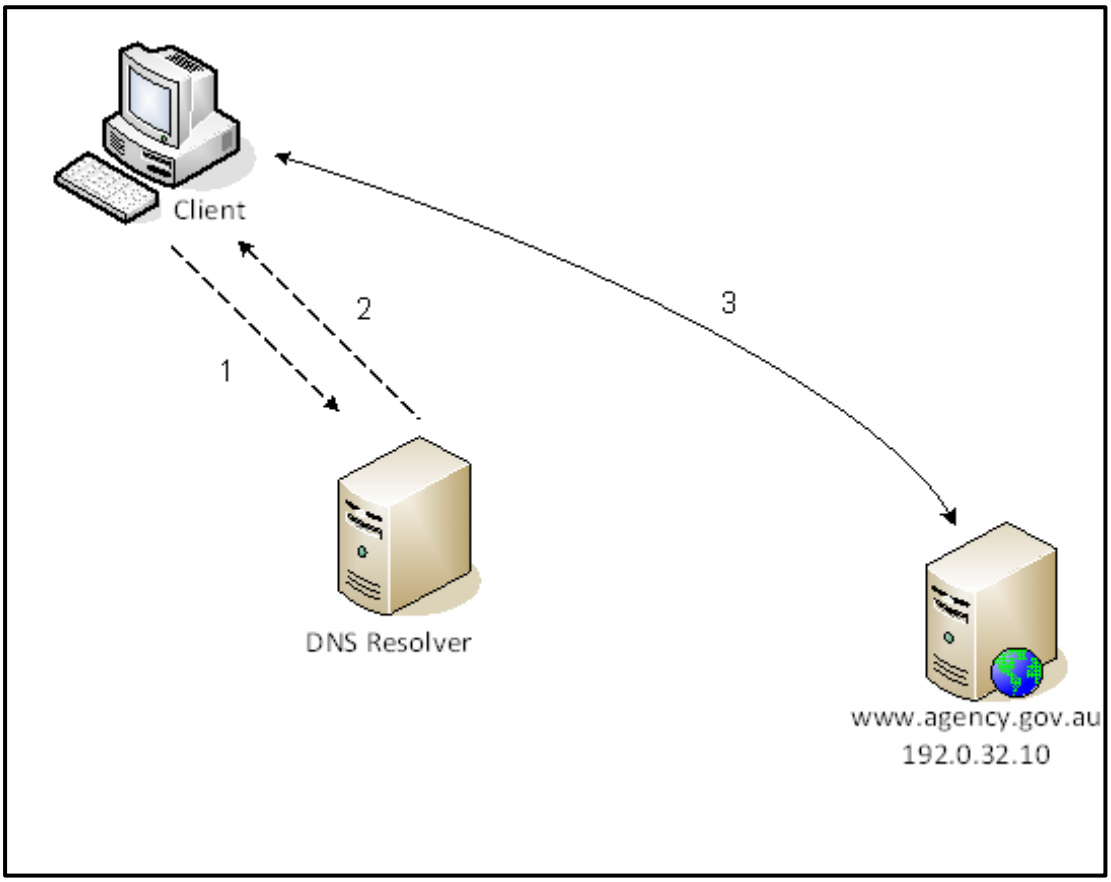

Figure 1: The normal DNS resolution process

1. Client queries DNS for the IP address of www.agency.gov.au.
2. DNS replies to client with IP address of www.agency.gov.au; 192.0.32.10
3. Client connects to 192.0.32.10; the IP address of www.agency.gov.au.

DNS spoofing

9. A DNS spoofing attack subverts the normal DNS resolution process as follows:

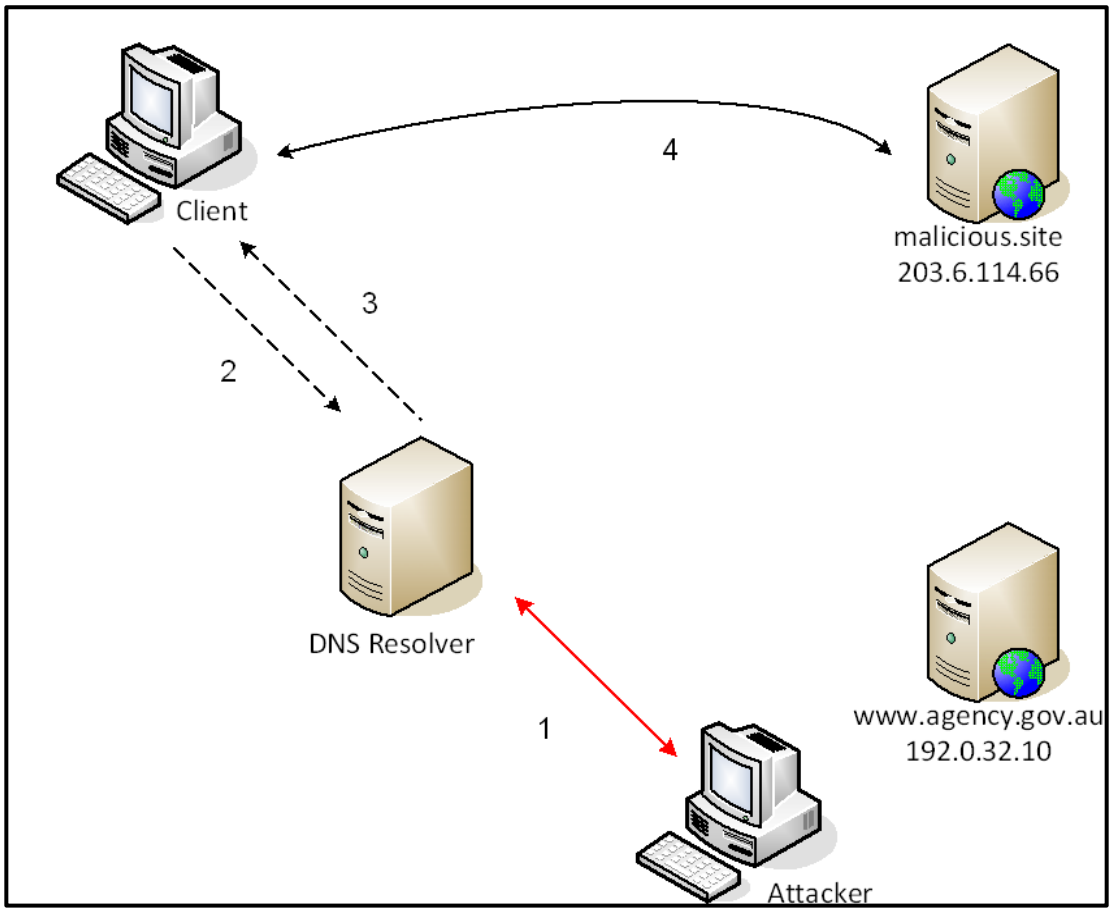

Figure 2: The normal DNS resolution process altered by DNS spoofing.

1. Cyber actor adds or alters DNS record for www.agency.gov.au on DNS resolver to point to 203.6.114.66 instead of 192.0.32.10.
2. Client queries DNS for the IP address of www.agency.gov.au
3. DNS replies to client with IP address of 203.6.114.66.
4. Client connects to malicious site 203.6.114.66. expecting it to be the genuine site for www.agency.gov.au

DNS cache poisoning

10. A DNS Cache poisoning attack subverts the normal DNS resolution process as follows:

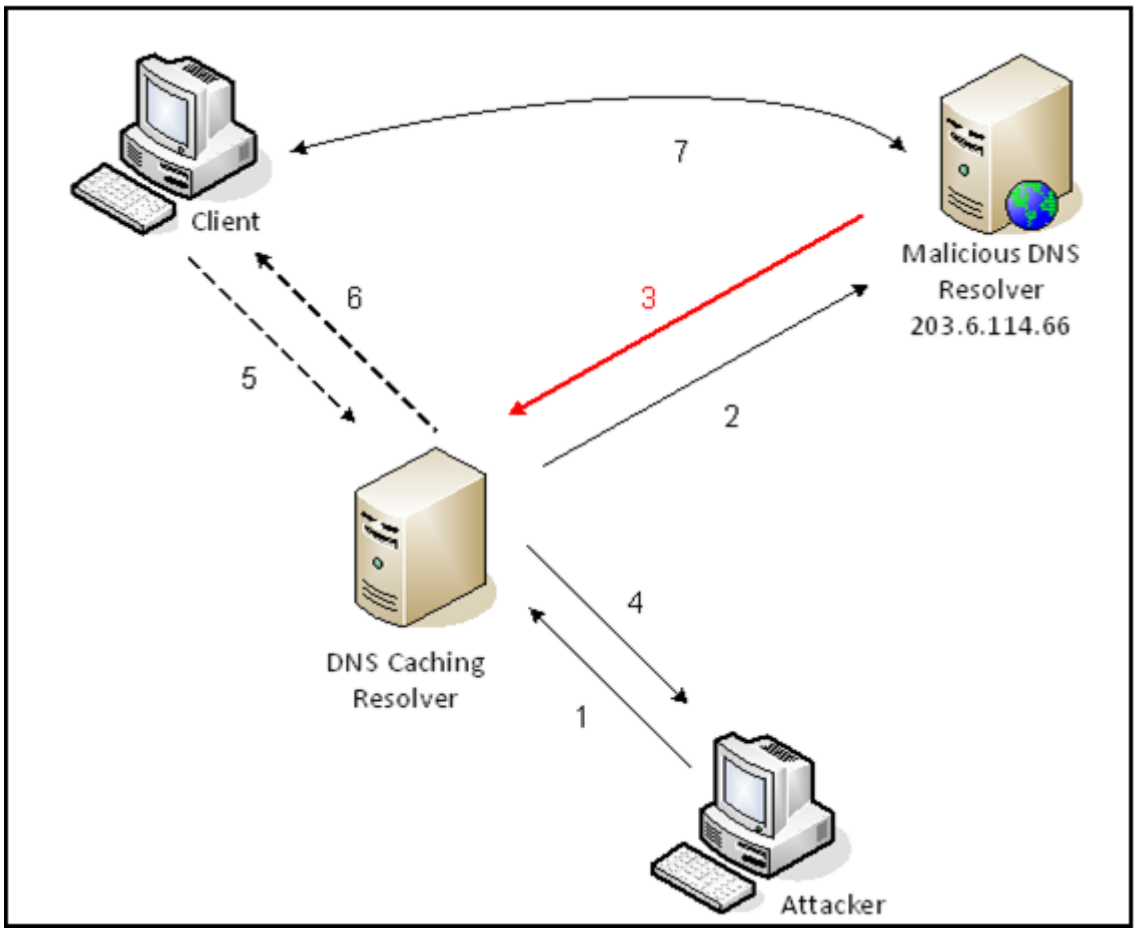

Figure 3: The normal DNS resolution process altered by DNS cache poisoning.

1. Cyber actor queries a DNS resolver for the IP address of a malicious site.
2. DNS resolver does not have the IP address and queries a malicious DNS resolver which has already established a relationship with the DNS resolver, see DNS Spoofing above.
3. Malicious DNS resolver provides requested IP address (203.6.114.66) along with falsified IP addresses for additional sites (e.g www.agency.gov.au.)
4. DNS resolver replies to cyber actor and caches the false IP addresses.
5. Client queries DNS for the IP address of www.agency.gov.au.
6. DNS resolver replies to client with (cached) IP address of 203.6.114.66.
7. Client connects to 203.6.114.66 expecting it to be the genuine www.agency.gov.au website.

DNS cache poisoning with flooding

11. A DNS Cache poisoning attack with flooding subverts the normal DNS resolution process as follows:

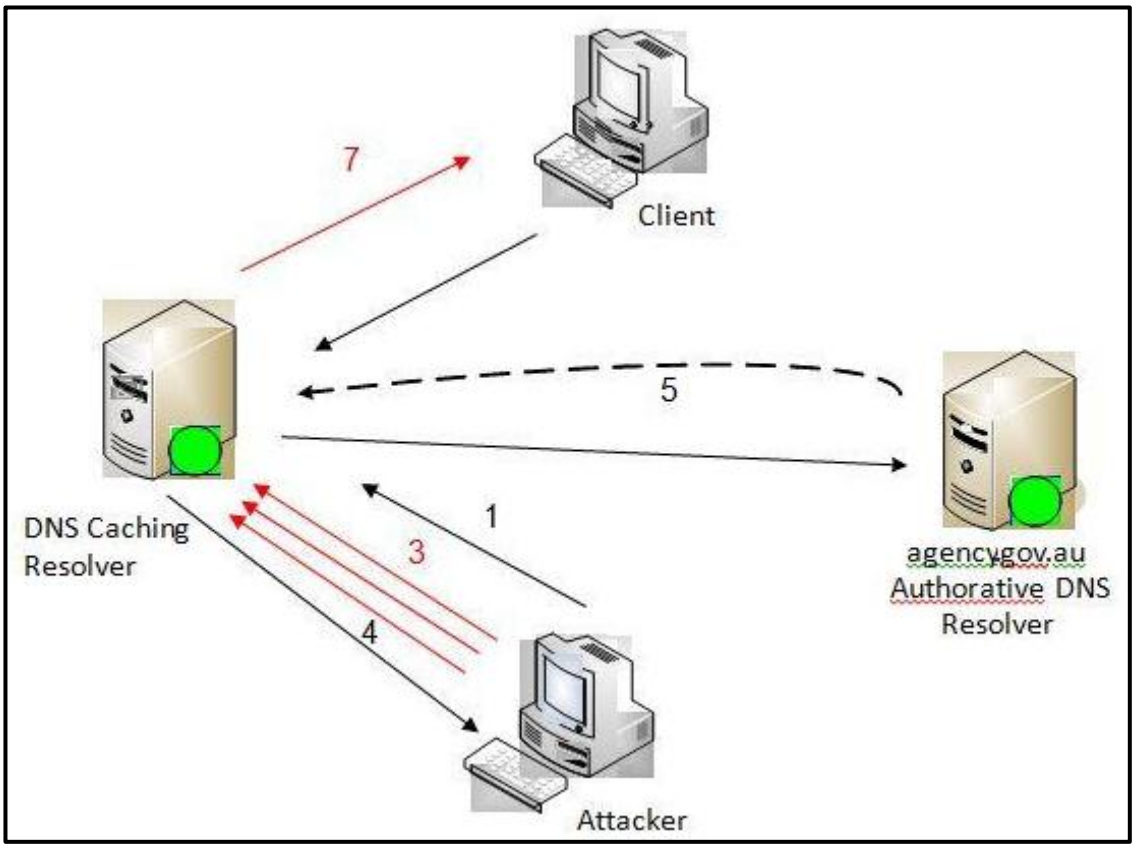

Figure 4: The normal DNS resolution process altered by DNS cache poisoning (with flooding).

1. Attacker queries DNS caching resolver for IP address of www.agency.gov.au
2. The DNS caching resolver queries the authoritative DNS server for www.agency.gov.au
3. The DNS caching resolver will accept the first response that matches the transaction ID and source port of its query to the authoritative server. The attacker floods the caching DNS resolver with fraudulent responses containing many different transaction IDs and source ports, hoping once of these will match.
4. One of the attacker's fraudulent responses is accepted. The DNS caching resolver responds to the attacker's original query with the poisoned result.
5. The authoritative DNS resolver responds to the DNS caching resolver. This response is ignored since the caching server already accepted a fraudulent response from the attacker.

6. A client tries to reach www.agency.gov.au and looks up the IP address of the site by querying the DNS caching server.
7. The DNS caching server returns a result from its cache which is the poisoned result provided by the attacker in 3. This poisoned result will direct the client to a malicious site.

Recommendations

12. Agencies should consider the following recommendations as part of their cyber security risk assessment process.

Apply the latest patches available for your DNS Resolver

13. DNS resolvers should have the latest security patches applied, as this reduces the opportunities for a cyber actor to leverage known vulnerabilities to exploit systems.

Separate Authorative and Recursive DNS Resolvers

14. Agencies should ensure that published authorative DNS servers, which are used by external parties to resolve www.youragency.gov.au, do not also resolve external domain names, such as www.google.com. The public authorative DNS resolver should only resolve hosts that your agency is responsible for and wishes to advertise.

15. Published agency DNS servers should not be configures to allow recursion. DNS severs configured in this manner permit external parties to masquerade as your agency when performing DNS queries – perhaps to inappropriate sites.

Limit Zone Transfers

16. Zone transfers permit all DNS information to be listed for a given domain and are a mechanism used by primary and secondary DNS resolvers to update DNS information. The default behaviour for DNS zone transfer permits any host to request and receive a full zone transfer for a domain.

17. Allowing open DNS Zone transfers is akin to an anonymous caller requesting and receiving your agency's complete telephone and address book. Information leakage form a seemingly innocent zone transfer could expose internal network topology that is useful to a cyber actor to do further harm.

Randomise source ports and Transaction Identifiers

18. Recursive (caching) DNS resolvers are used by internal clients to resolve external addresses. They should use random source ports and random transaction IDs to reduce the likelihood of a cyber actor successfully guessing and faking a response designed to poison the cache of your DNS resolver.

19. Avoid using routers, firewalls and other gateway devices that perform Network Address Translation (NAT), or more specifically, Port Address Translation (PAT) on DNS traffic. PAT devices often rewrite source ports to track connection state, thus negating the effect of any randomisation implemented by DNS.

Outsource

20. Agencies should consider outsourcing DNS management as an available risk treatment option once they have conducted an IT security risk assessment. DNS can be inherently complex, and requires considerable effort to maintain securely. Services are commercially available and can offer advantages such as Business Continuity and increases to service availability and security of DNS resolvers.

References and further information

[1] http://www.kb.ccrt.org/vyls/id/800113

[2] http://www.cert.org/archive/pdf/dns.pdf

[3] http://www.technicalinfo.net/papers/Pharming.html

[4] https://media.blackhat.com/bh-usa-08/video/bh-us-08-Kaminsky/black-hat-usa-08-kaminsky-blackops08-hires.m4v

[5] http://www.blackhat.com/presentations/bh-dc-09/Wouters/BlackHat-DC-09-Wouters-Post-Dan-Kaminsky-slides.pdf

[6] http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf

[7] http://www.dnssec.net

[8] https://members.onsecure.gov.au/q=node/141770

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.