Australian Government
Australian Cyber Security Centre

ACSC
AUSTRALIAN CYBER SECURITY CENTRE

PROTECT

AUGUST 2012

Domain Name System Security

Introduction

1. This publication provides information on Domain Name System (DNS) security. DNS systems, known as DNS Resolvers, are vulnerable to a number of exploits that can lead to compromises. This publication provides information on protecting DNS integrity and mitigation strategies to reduce the likelihood of DNS Resolver compromises.

2. Organisations are recommended to implement the mitigation strategies in this publication as a priority. Following the mitigation strategies will help to ensure that users are directed to genuine websites 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 Internet Protocol (IP) addresses and vice versa.

Background

4. DNS has no authentication mechanisms included by default. The lack of authentication increases the risk of falsified DNS information being stored on a DNS Resolver by entities with no authority to do so. These activities are known as DNS spoofing and DNS cache poisoning.

5. DNS spoofing and DNS cache poisoning can permit an adversary to map the internal network of an organisation 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 a DNS record 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 to allow external access permits entities to masquerade as an organisation when performing DNS queries – perhaps to inappropriate websites.

Normal DNS resolution

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

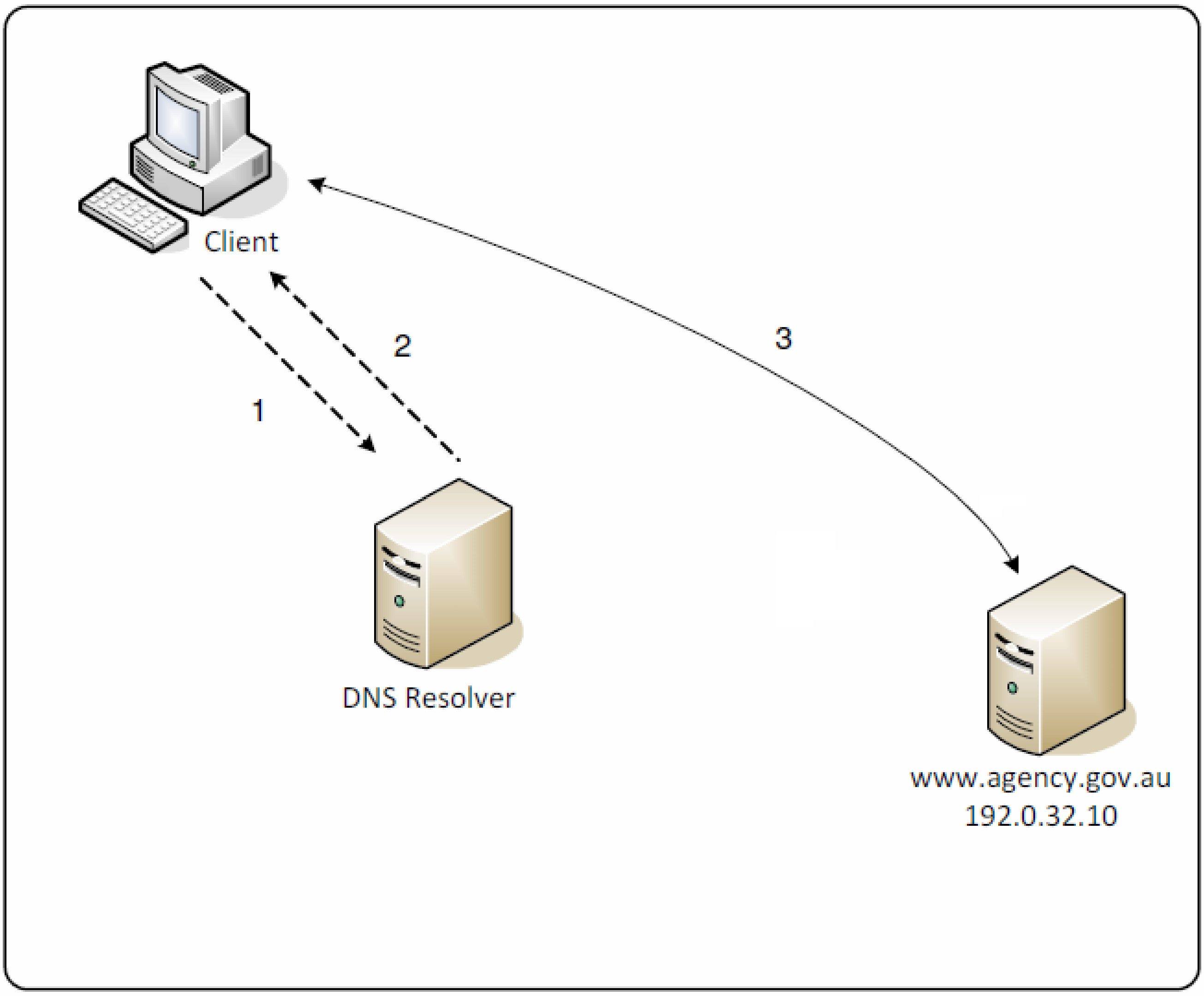

Figure 1: The normal DNS resolution process

(1) The client queries a DNS Resolver for the IP address of www.agency.gov.au.

(2) The DNS Resolver replies to the client with the IP address of 192.0.32.10.

(3) The 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.

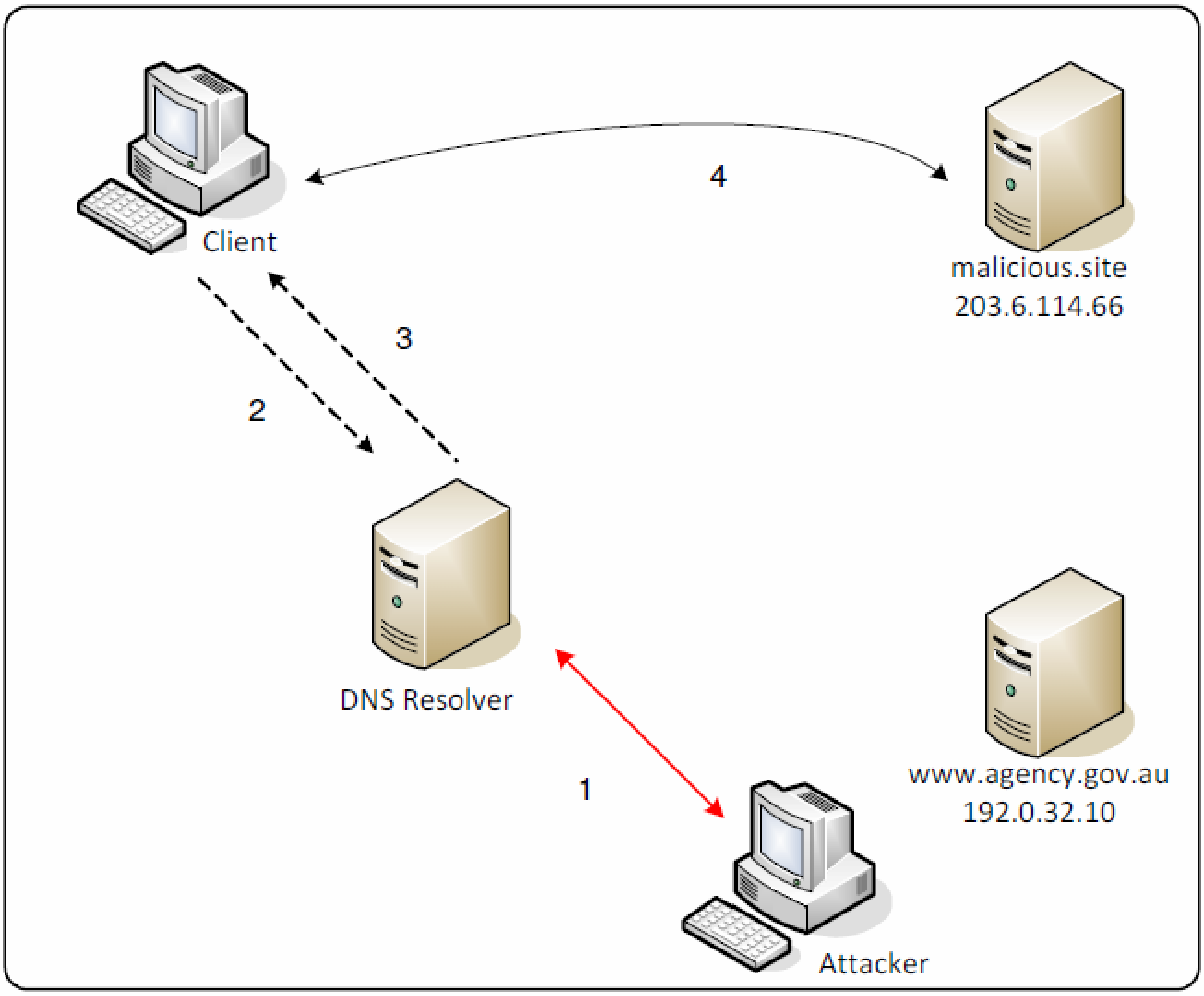

Figure 2: The normal DNS resolution process altered by DNS spoofing

(1) An attacker adds or alters the DNS record for www.agency.gov.au on the DNS Resolver to point to 203.6.114.66 instead of 192.0.32.10.

(2) The client queries the DNS Resolver for the IP address of www.agency.gov.au.

(3) The DNS Resolver replies to the client with the IP address of 203.6.114.66.

(4) The client connects to 203.6.114.66 expecting it to be the IP address of www.agency.gov.au.

DNS cache poisoning

10. A DNS cache poisoning attack also subverts the normal DNS resolution process.

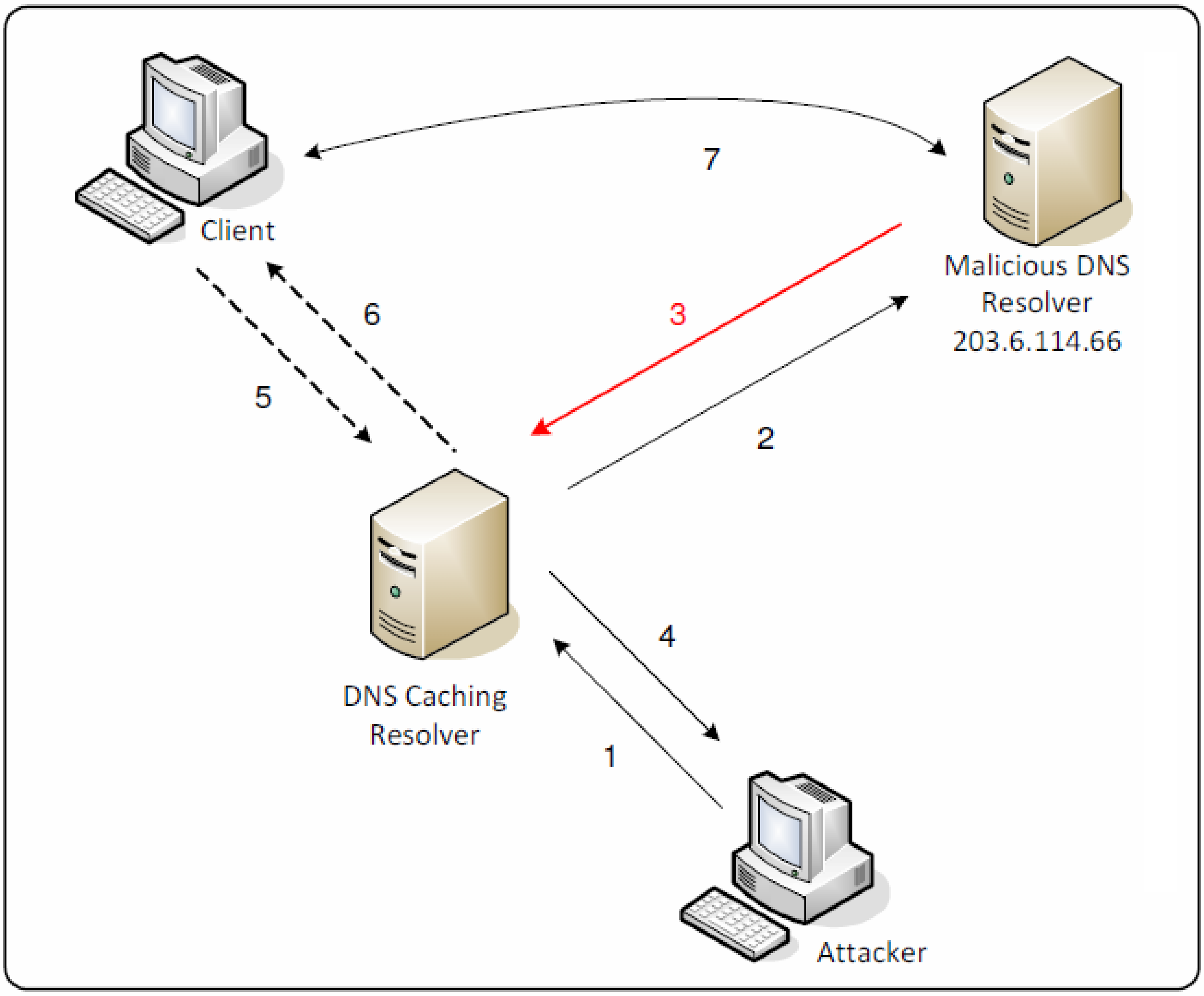

Figure 3: The normal DNS resolution process altered by DNS cache poisoning

(1) An attacker queries a DNS Caching Resolver for the IP address of a malicious website.

(2) The DNS Caching Resolver does not have the IP address and queries a malicious DNS Resolver which has already established a relationship with the DNS Caching Resolver via DNS spoofing.

(3) The Malicious DNS Resolver provides the IP address of 203.6.114.66 along with falsified IP addresses for additional websites (e.g. www.agency.gov.au).

(4) The DNS Caching Resolver replies to the attacker and caches the false IP addresses.

(5) The client queries the DNS Caching Resolver for the IP address of www.agency.gov.au.

(6) The DNS Caching Resolver replies to the client with the cached IP address of 203.6.114.66.

(7) The client connects to 203.6.114.66 expecting it to be the IP address of www.agency.gov.au.

DNS cache poisoning with flooding

11. A DNS cache poisoning attack with flooding also subverts the normal DNS resolution process.

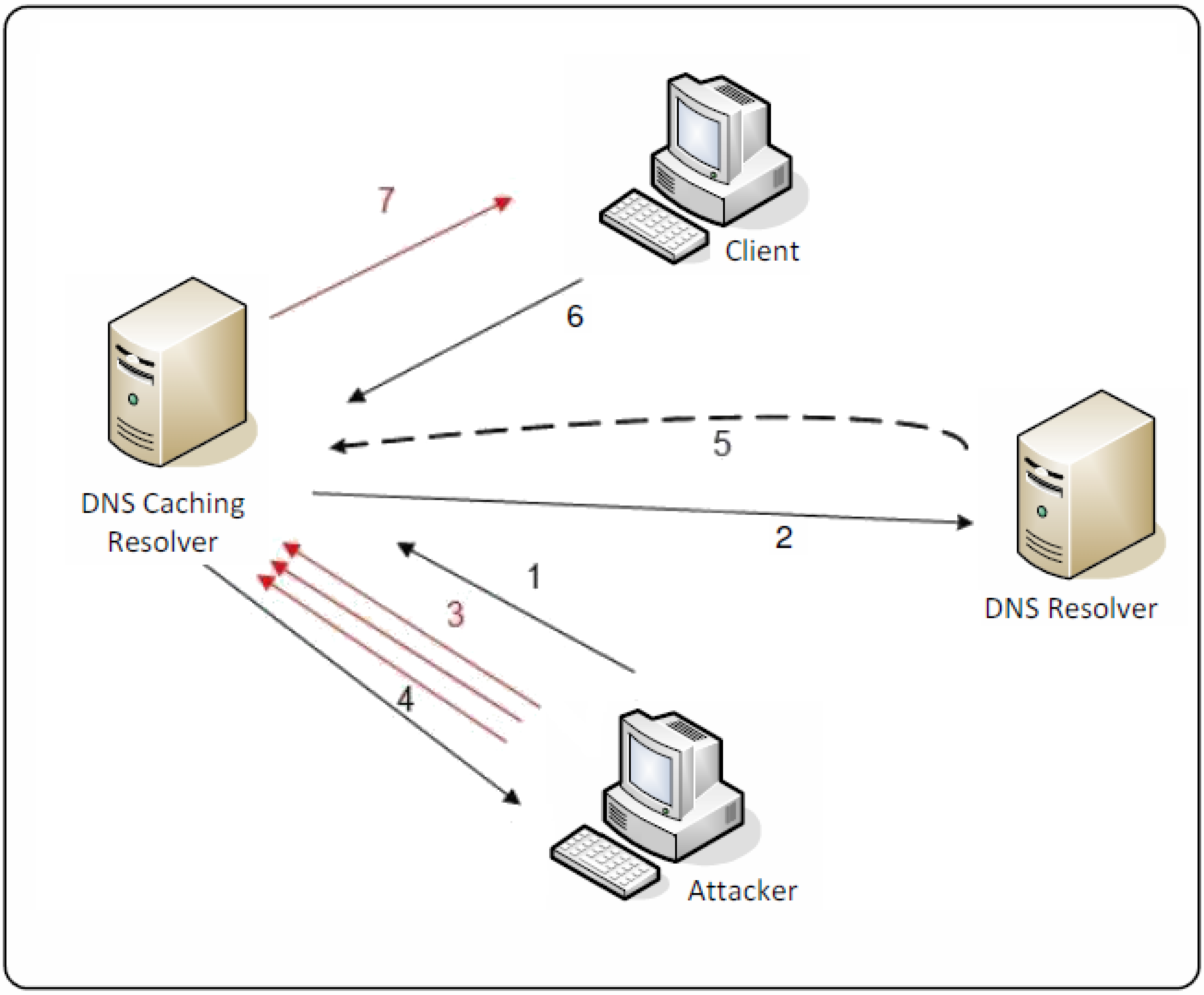

Figure 4: The normal DNS resolution process altered by DNS cache poisoning with flooding

(1) An attacker queries a DNS Caching Resolver for the IP address of www.agency.gov.au.

(2) The DNS Caching Resolver queries an authoritative DNS Resolver 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 DNS Resolver. As such, the attacker floods the DNS Caching Resolver with fraudulent responses attempting to match the transaction ID and source port it is expecting.

(4) Once the attacker's fraudulent response is accepted, the DNC Caching Resolver responds to the attacker's original query with the poisoned result.

(5) The authoritative DNS Resolver responses to the DNS Caching Resolver. However, this response is ignored since the DNS Caching Resolver had already accepted the fraudulent response from the attacker.

(6) The client queries the DNS Caching Resolver for the IP address of www.agency.gov.au.

(7) The DNS Caching Resolver replies to the client with the poisoned IP address provided by the attacker thereby directing them to a malicious website.

Mitigation strategies

12. Organisations should consider the following mitigation strategies to reduce the likelihood of DNS Resolver compromises.

Apply the latest patches for DNS Resolvers

13. DNS Resolvers should have the latest security patches applied as this reduces the opportunities for an adversary to leverage known security vulnerabilities to exploit them.

Separate authoritative and recursive DNS Resolvers

14. Organisations should ensure that published authoritative DNS Resolvers, 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 authoritative DNS Resolver should only resolve hosts that your organisation is responsible for and wishes to advertise.

15. Published organisation DNS Resolvers should not be configures to allow recursion. DNS Resolvers configured in this manner permit external entities to masquerade as your organisation when performing DNS queries – perhaps to inappropriate websites.

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 organisation’s complete telephone and address book. Information leakage form a seemingly innocent zone transfer could expose internal network topology that is useful to an adversary.

Randomise source ports and transaction Identifiers

18. DNS Caching Resolvers are used by internal clients to resolve external domains. They should use random source ports and random transaction IDs to reduce the likelihood of an adversary successfully guessing and faking a response designed to poison the cache of a 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

Organisations should consider outsourcing DNS management. DNS can be inherently complex and requires considerable effort to maintain securely. Services are commercially available and can increase service availability and security of DNS Resolvers.

Further information

20. Additional information on DNS can be obtained from the following websites:

    a. https://csrc.nist.gov/publications/detail/sp/800-81/2/final

    b. http://www.dnssec.net

    c. http://www.technicalinfo.net/papers/Pharming.html

    d. https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf

    e. https://www.blackhat.com/presentations/bh-dc-09/Wouters/BlackHat-DC-09-Wouters-Post-Dan-Kaminsky.pdf.

Contact details

21. Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).