Utility Regulation and Competition Office

OfReg
PO Box 2502
Grand Cayman, Cayman Islands
KY1-1104
Tel: (345) 946-4282
Fax: (345) 945-8284

PRESS RELEASE FROM THE UTILITY REGULATION AND COMPETITION OFFICE OF THE CAYMAN ISLANDS

OFREG HIGHLIGHTS IMPORTANCE OF DOMAIN NAME SYSTEM SECURITY EXTENSIONS FOR DOMAIN NAME INDUSTRY

GRAND CAYMAN, CAYMAN ISLANDS, 27 MARCH 2019

OfReg is today publishing a notice, remining of the dangers of cyberattacks on the domain name system (DNS), and publishing links to further advice on preventing such attacks. This advice is aimed at members of the domain name industry, such as registries, registrars, resellers as well as networks operators which operate DNS data requests.

Attacks on the DNS typically involve unauthorised changes to records in the DNS system, so that a request to access DNS data results in a user being routed to an alternative IP address.

When a user enters a web address, the browser uses a stub resolver to request DNS data from a recursive resolver, which itself sends a query to an authoritative name server (ANS) for the DNS data. The DNS data response from the ANS cannot itself be verified, and therefore is open to manipulation through malicious attack. Recursive resolvers relating manipulated DNS data back to the stub resolver results in a user being directed to an alternative IP address. For this reason, these attacks are sometimes called domain hijacks.

As a result of these attacks users can, for example, unwittingly be redirected to replica banking websites where user credentials can be stolen. DNS settings can also be manipulated so that emails can be received and stored by someone other than the intended recipient.

Such attacks are of concern to network operators since they may run recursive resolvers to process DNS requests, sent by devices on their network.

ICANN (Internet Corporation for Assigned Names and Numbers) has recently called for full deployment of the Domain Name System Security Extensions (DNSSEC) which strengthens authentication of DNS data by using digital signatures. However, DNSSEC must be specifically enabled by DNS industry actors.

OfReg is urging all members of the domain name industry to ensure their systems are protected, and to enact robust security policies to protect data. Further information can be found at the links below.

ENDS

There is more information about DNS and DNSSEC at the ICANN website

In February ICANN published a checklist of recommended security precautions for DNS industry actors, including network operators.