NATIONAL BANK
Deimon Tencio

1. DNS is a very important piece on the Internet; and today we have confident when we perform a query to a Web site from our browser. Example is when we write in our browser the URL www.bnonline.fi.cr and our browser displays the web site to conduct transactions. But that would happen if this technological system is exposed as Mr Kaminsky has declared at the Blackhat Conference? What if would happen if our DNS queries provide us with false network address re-direct to a fake website, or re-direct our mail to a wrong site or relying on patches update sites or down fake software?

2. For hackers banks are one of the largest centers of attention as they seek to exploit vulnerabilities, to make transactions that mobilize millionaires amounts to be extracted, therefore Phishing methods used to set up fake sites that capture the information from the customer to then use to authenticate to the actual site. Phishing is one of the most common banks in Costa Rica attacks and to exploit it, used the sending of emails requesting customer click the attached link, which re-direct them to false pages showing a duplicate the Bank, thus fooling the customer.

3. That is why banks have implemented security mechanisms to counter such attacks, inside of which are the use of several factors authentication mechanisms, as well as educate customers care to verify the URL and do not respond to suspicious emails; However, the attacks continue to be improved and focused on the resolution of names. One of them is the Pharming attack, which poisons the host the client PC or the DNS which consulted the client.

4. There are several strategies that have been used for this attack, the installation of fake DNS and the diversion of the client computers to the fake DNS through scripts introduced through malware (DNS Changer). That regardless of that the possibility of an internal attack which poison the cache of the DNS of the company, the bad handling of DNS internal staff and people who manipulate the network and are introduced in the middle of it there is.

5. Therefore the implementation of DNSSEC brings several benefits, such as greater confidence in the navigation, security to the sending of e-mail; avoid fraudulent sites and progress in new security mechanism using the authentication of the consultations. (An example would be the development of applications that exploit the DNS authentication to verify the origin and destination of the mails)

6. For this reason the Bank has been keen to implement DNSSEC in one of their transactional domains, in order to provide the customer with greater confidence and security in the income of the banking services.

7. Finally, I believe that a key point in this will be the explorers that people use, that they must be able to show the user which you DNS query was made with safe and reliable domain, signatures to validate the DNSSEC. Another important point is implementing DNSSEC in the DNS, because as we left with security in some domains and others not.