Lesson from a Security Incident

Luis Diego Espinoza
NIC - Internet Costa Rica

ICANN 41 - Singapore
19 - 24 June 2011

.cr
NIC-Internet Costa Rica
Academia Nacional de Ciencias

Registro de dominios bajo .cr

Agenda

- The incident.
- Dissection of the incident.
  - Data affected.
  - How the hacker did it.
  - Vulnerability.
- Lesson learned.

About NIC

- In 1990 IANA assigns the ccTLD .CR to National Academy of Sciences (ANC).
- The ANC create the administrative NIC Internet, to manage the ccTLD.
- The ANC is part of National System of Science and Technology supported by Ministry of Science and Technology.

NIC-Internet Costa Rica
Academia Nacional de Ciencias

Registro de dominios bajo .cr

The incident

- January 17th 2011: The Operation Manager reports changes in some high value domains made by a different user account.
- We shutdown the server immediately
- Few hours later we bring up the site with IP based restrictions for the management interface.

Data affected

- Some information on 6 high value domains on January 15th 2011, 4:28am
- 24 administrative transactions.
- None of the changes went to DNS tables.
- We can revert all the changes.

NIC-Internet Costa Rica
Academia Nacional de Ciencias

Registro de dominios bajo .cr

How the intruder did it

- The intruder used valid customer user id (NIC-Handle) with a valid password.
- The intruder used valid management username and password to approve the changes.
- The intruder obtained information about users from logs in the web server.

About vulnerabilities

- Since 2009 we started to review possible threats in the web site from sans.org and owasp.org, including SQL Injection. An email from Yuri Ito to the ccNSO mailing list, alert us.
- We are aware of possible social engineering attacks with employees, then we look for trusted people when hire.
- We are aware of possible mistakes in the technical management, then we have additional controls to verify some changes.

About vulnerabilities

- Some controls it can't be stablished in that moment, like security source code review, or penetration tests, because there's not enough technical resources.
- The security is an improve cycle that never ends, then it is impossible to have all the vulnerabilities covered.

What the intruder did

- Login in to the customer portal trying some valid NIC-Handles and passwords.
- Request changes in some domains.
- Login in to the management portal and approve the changes. (Reject the first one!)
- Request some changes in domains from management portal.

NIC-Internet Costa Rica
Academia Nacional de Ciencias

Registro de dominios bajo .cr

Transactions

Domain	Time	Transaction	Login users
1	15/01/2011 04:10:56 AM	DNS Servers	Customer portal: client-1@nic-handle – Mgt Portal: internaluser
1	15/01/2011 04:15:01 AM	DNS Servers	Customer portal: client-1@nic-handle – Mgt Portal: internaluser
2	15/01/2011 04:28:27 AM	Approve	Customer portal: client-1@nic-handle – Mgt Portal: internaluser
2	15/01/2011 04:33:32 AM	Reject	Customer portal: client-1@nic-handle – Mgt Portal: internaluser
2	15/01/2011 05:29:24 AM	Approve	Customer portal: client-1@nic-handle – Mgt Portal: internaluser
3	15/01/2011 05:44:27 AM	DNS Servers	Customer portal: client-1@nic-handle – Mgt Portal: internaluser
3	15/01/2011 05:56:24 AM	DNS Servers	Mgt Portal: internaluser
1	15/01/2011 06:03:45 AM	DNS Servers	Mgt Portal: internaluser
3	15/01/2011 06:40:15 AM	DNS Servers	Mgt Portal: internaluser
1	15/01/2011 06:48:39 AM	DNS Servers	Mgt Portal: internaluser
1	15/01/2011 06:50:19 AM	DNS Servers	Mgt Portal: internaluser
1	15/01/2011 06:52:00 AM	DNS Servers	Mgt Portal: internaluser
1	15/01/2011 06:59:37 AM	Domain Contacts	Mgt Portal: internaluser
1	15/01/2011 07:07:37 AM	Domain Contacts	Mgt Portal: internaluser
1	15/01/2011 07:08:23 AM	DNS Servers	Customer portal: deneme3@hotmail.com.tr – Mgt Portal: internaluser
1	15/01/2011 07:18:21 AM	Domain Contacts	Mgt Portal: internaluser
4	15/01/2011 08:33:10 AM	Domain Contacts	Mgt Portal: internaluser
4	15/01/2011 08:34:16 AM	DNS Servers	Customer portal: deneme3@hotmail.com.tr – Mgt Portal: internaluser
4	15/01/2011 08:36:40 AM	Domain Contacts	Mgt Portal: internaluser
1	17/01/2011 09:08:25 AM	DNS Servers	Customer portal: client-1@nic-handle – Mgt Portal: internaluser
3	17/01/2011 11:23:00 AM	DNS Servers	Customer portal: client-1@nic-handle – Mgt Portal: internaluser2
5	17/01/2011 11:30:22 AM	DNS Servers	Mgt Portal: test
6	17/01/2011 12:45:17 PM	Domain Contacts	Mgt Portal: internaluser
6	17/01/2011 12:58:07 PM	DNS Servers	Mgt Portal: internaluser
6	17/01/2011 12:59:00 PM	DNS Servers	Mgt Portal: internaluser

Obtaining usernames and passwords

- Not reveled by an employee.
- Not brute-force attack.
- Not SQL Injection, but did try.
- In fact it was obtained from logs from the misconfigured web server allowing directory listing.
- The misconfiguration was detected and corrected one month before the attack.

Vulnerability exploited

- Our software developer write the passwords on the log files.
- A temporary misconfiguration of the web server allow to read log files. This was corrected one month before the intruder try to make changes.
- The intruder learn how works our internal registration process.

Collateral damage

- In this case, the DNS data was never altered and this high value domains was not affected on the DNS, BUT
- The system sent emails to the contact every time that there is a change in their domains, creating an alert on that costumers.
- Affect our image.

Things to think about

- Fortunately, our automation development was late, then wasn't automation at that moment, we could stop the changes to the DNS before it causes more damages.
- There's a hugh challenge to improve the controls of transactions and try to implement the criteria of the human in the automation.

Took actions

- Force expiration of all passwords in the system.
- Implement access to the management portal exclusively through a VPN Tunnel and IP based access list.
- Source code review by third party (me :-)) of all new developments and improves in the system.

Learned lessons

- The chain was broken at the weakest link! We need to reinforce that links.
- Test, test, test. We need to improve the security testing in all steps. Penetration test, code review for vulnerabilities.
- Used to focus on security and stability of the DNS resolution process, but we need to pay more attention to the web system too.

Learned lessons

- We need to implement automation of alerts using complex criteria to try to cover the common sense of the human detection of possible problems. (If it is possible!)

Thanks! Questions?

.cr
NIC-Internet Costa Rica
Academia Nacional de Ciencias

Registro de dominios bajo .cr