MarkMonitor®

PUERTO RICO Top Level Domain

Domain System Threat Landscape

Pablo Rodriguez – Nic.pr

Janelle McAlister - MarkMonitor

Agenda

- History
- Nic.PR Case Study
  - Registrar Perspective
  - Registry Perspective
- Future solutions

History

- Over the past few years multiple ccTLD registries and registrars have been attacked leading to the defacement of high profile domain names.

Domain Name Security Breaches on the Rise

- Individuals now more than ever, recognize that domain security can be breached
- Registries and registrars are exploited as technical and social vulnerabilities are uncovered

Targeting Domain Related Vulnerabilities

- Infrastructure Breaches
- Process Exploits

Registry

- Social Engineering Attacks
- Infrastructure Breaches

DNS Provider

- Social Engineering Attacks
- Domain Hijackings
- Infrastructure Breaches

Registrar

DNS Administrator

Domain Administrator

- Credential Theft
- Identity Theft

Who Plays a Part in Increasing Domain Security?

- Registrants
- Registrars
- Registries

PUERTO RICO
Top Level Domain

Domain System Threat Landscape

Incident Description

- April 26, 2009: At approximately 9:00 AM we identified that google.com.pr had been attacked.
- The event triggered an assessment of our entire database and we found that other domain names were compromised as well.
- The attacks came from the self proclaimed Turkish group Peace Crew.

Google Puerto Rico Hacked !

Agd_Scorp & Thehacker

rx5 & Cr@zy_King & BLaSTeR

[root@markmonitor:/Peace-Crew] # is back
[root@markmonitor:/Peace-Crew] # your system get down.!

Avlanma Zamani !

Thx: Kerem125, Jextoxic , S3f4, Redrolix, Kacak

Microsoft New Zealand Hacked by Peace Crew

Aaaare youuuu Hackeeeed !!

Agd_Scorp - rx5 - Cr@zy_King

JeXToXiC 4R!F KacaK BLAsteR Cebrail AmeN

Zec TheHacker ZeberuS s3f4 Frabtyy NetRoot Suskun

PAKbugs Crew Friends :Zombie_KSA spo0fer xOOmxOOm

unutkularimiz affede..

STOP THE WAR ISRAEL

IID in the news

ActiveInterest blog

ActiveFeed news

Domain hijacked after registrars hacked in Puerto Rico and New Zealand

Written by Lars Harvey

Wednesday, 29 April 2009 00:00

In separate incidents just days apart, a group calling itself "Peace Crew" hacked into the domain management systems at DomainZ and Nic.pr. The hackers changed the DNS settings for domains owned by several major brands in the .PR (Puerto Rico) and .NZ (New Zealand) ccTLD domain spaces, then redirected the hijacked domains to simple defacement-type web pages. The hacked websites carried the messages: "Hacked by Peace Crew" and "STOP THE WAR ISRAEL". On the Microsoft domains, the hackers added a picture of young Bill Gates sporting the remnants of a cream pie on his face.

DomainZ was attacked on April 21, 2009, followed by Nic.pr getting attacked on April 26. In both cases, the hackers used SQL injection techniques to exploit the domain administration panel on the registrars' systems. The list of brands whose domains were hijacked includes BitDefender, Coca-Cola, Dell, F-Secure, Google, HSBC, Microsoft, Nike, Nokia, PC World, Sony, Symantec, Xerox, and Yahoo.

SECURITY Jan 9, 2009 4:30 pm

Hackers Deface NATO, US Army Web Sites

By Robert McMillan, IDG News

Hackers have taken down two high-profile targets as they continue their ongoing Web attacks in support of Palestine, defacing Web sites run by the U.S. Army and the North Atlantic Treaty Organization (NATO).

SIMILAR ARTICLES:

Got $500? You Can Buy a Hacked U.S. Military Website

Hacked iTunes Accounts Continue to Sell in China

Twitter Targeted With Fake Antivirus Software Scam

IBM DeveloperWorks Site Defaced

WikiLeaks Avengers Threaten UK Government Sites

Congressional Web Sites Hacked Near Obama Speech

The attacks on Thursday took down the Web sites for The United States Army Military District of Washington and the NATO Parliamentary Assembly, according to Zone-H, a Web site that tracks defacement activity.

The NATO site is now back online, but the U.S. Army site was still offline Friday morning. A version of the Web page cached by Google reads: "Stop attacks u israel and usa ! you cursed nations ! one day muslims will clean the world from you ! " NATO didn't immediately respond to a request for comment.

Most other U.S. Army sites do not appear to have been affected by that attack. The U.S. Army Military District of Washington is an army command, based in Fort Lesley J. McNair in Washington, D.C.

Using what's known as a SQL injection attack, the group also defaced the Web site of the Joint Force Headquarters of the National Capital Region, which handles military incident response for the Washington, D.C., area, according to Gary Warner, director of research in computer forensics with the University of Alabama at Birmingham. A U.S. Army spokeswoman was unable to immediately comment on reports of the hacks.

All of these attacks are credited to a Turkish hacking group called Agd_Scorp / Peace Crew.

Compromised Domain names

coke.com.pr	microsoft.pr
coca-cola.com.pr	msn.pr
hotmail.com.pr	microsoft.com.pr
msn.com.pr	hsbc.com.pr
passport.com.pr	google.com.pr
fanta.com.pr	gmail.pr
fanta.net.pr	paypal.com.pr
fanta.org.pr	gmail.com.pr
nike.com.pr	nokia.com.pr
live.com.pr	pcworld.com.pr
nike.pr	yahoo.com.pr
norton.com.pr	youtube.pr
coca-cola.pr	nokia.pr
norton.pr	yahoo.pr

The Attack

- The attack consisted of an SQL Injection to our web-interface.
  - Username = 'or'=1
  - Password = 'or'=1

- The hackers were able to login to the web-interface of any client that he or she desired.

The Attack

- The hacker bypassed our interface login authentication/authorization mechanism.

- Once inside, the hackers changed the name servers of the compromised domain names and pointed them to their own name servers.

Vulnerability

- The code accepted cross-site scripting and did not made any user input validation for SQL Injections.
- Automatic domain name modifications were allowed without additional validation.
- Passwords were stored in clear text.
- Agglutinators and individuals authentication and validation used the same entry point.

Our Response

- The web-interface was locked down; thus, interrupting all login activities at the time.
- A backup database was uploaded to revert the changes made by the hacker.
- During this period of time changes to any account had to be requested via phone or email.
- The attack was contained 2 hours later.

Long Term Security Measures

- The code was updated with a set of functions for input validation and regular expressions.
- Registrars (agglutinators) and registrants (individuals) exist in segregated databases and servers.
- Likewise, segregated point of entries were created for registrars and registrants. The registrars' web-interface was enhanced with additional security features.

Long Term Security Measures

- Automatic changes were not allowed. Account modifications requests were confirmed with the admin or tech contacts, who had to approve or reject the changes via email.

- Registrars were requested to login to their interface either with a token (provided by us) or from a dedicated IP address.

- A custom Application Log was developed to aid in system monitoring.

Long Term Security Measures

- Agglutinators and individuals were issued new passwords.
- The passwords were generated employing a double encryption method.

Registrar Perspective

- During the incident with NIC.PR, MarkMonitor was able to contact the registry immediately.
- As registrar's, having after hours contact information for registries is critical in order to immediately respond to security issues.

Securing Domain Related Vulnerabilities

- Early Detection
- Ability to Quickly Respond
- Account Lock
- Registry Domain Lock

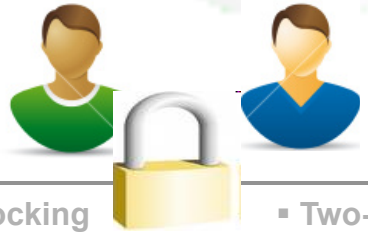
Registry

- Operational Policies
- Hardened Infrastructure
- Two-Factor Authentication
- IP Address Restrictions

DNS Provider

- Operational Policies
- Third-Party Evaluations
- Hardened Infrastructure
- Two-Factor Authentication
- IP Address Restrictions
- Portal Locking
- Registry Locking

Registrar



DNS Administrator

Domain Administrator

- Portal Locking
- Registry Locking

- Two-Factor Authentication
- IP Address Restrictions

Online Account Security

- Restricts access to Registrar's online Registry accounts based on their IP address range
- Lock all accounts if someone incorrectly enters the password more than 3 times
- 2-Factor (Token) log-in

Registry Lock

- The Registry removes the ability to update a domain name through the standard channels – i.e., online account or email templates.
- This is used for high profile, high traffic and/or mission critical domains.
- MarkMonitor has been working with both gTLD and ccTLD registries to implement this process.

Registry Lock

- Sample Process:
  - Domain names are only unlocked via a phone call between an authorized person from the Registrar and an authorized person from the Registry.
  - The authorized person from the Registrar must provide a secure passcode to unlock the domain.
  - Once the domain is unlocked the Registrar will follow the normal process to update the domain.
  - Once the domain is modified the authorized person from the Registrar will call the registry to relock the domain.

Questions??