How to Handle Domain Hijacking Incidents (Prevention, Investigation and Recovery)

Salman Niksefat, Mehdi Shajari,

APA Center, Amirkabir University of Technology

Supported by Iran Telecommunications Research Center(ITRC)

Tehran, Iran

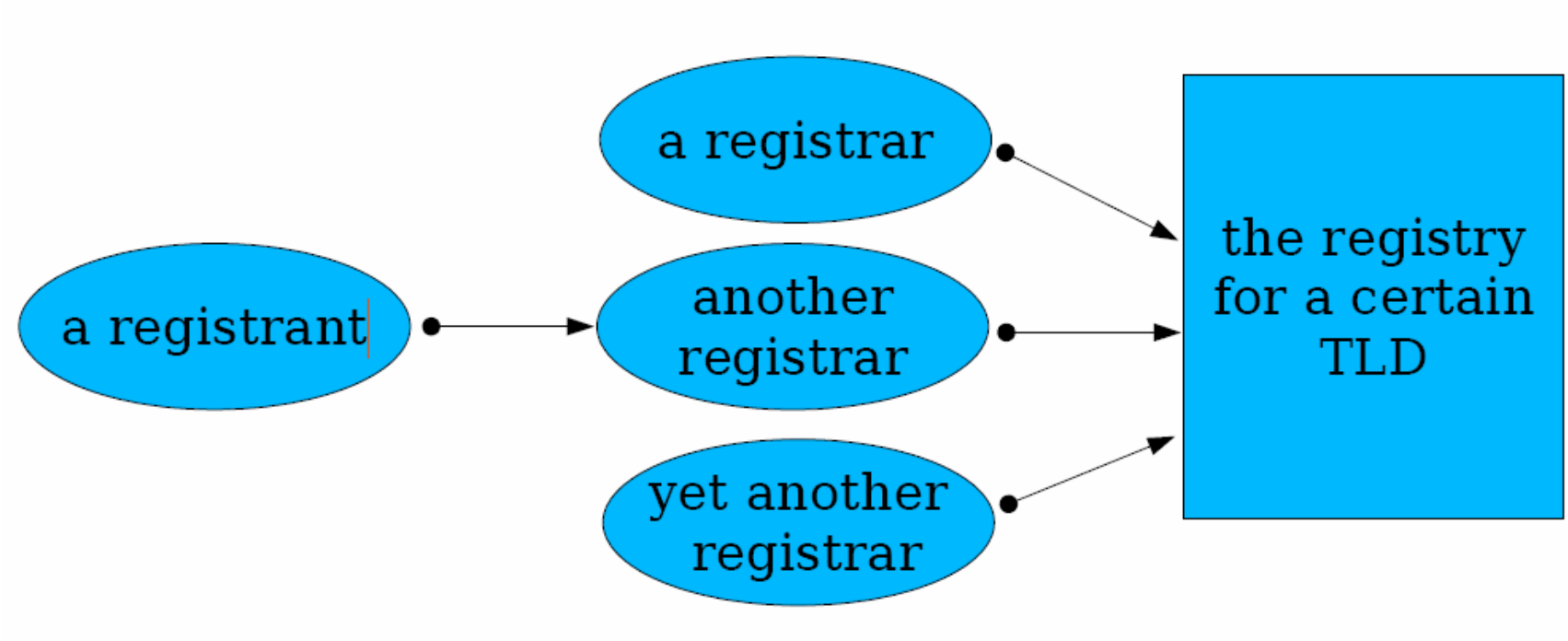
Overview

- Terms
- Definition of Domain Hijacking
- Who are affected?
- Effects and Damages
- Motivations for hijackers
- How is it done?
- How to prevent?
- How to investigate?
- How to recover?
  - UDRP Standard Policy
- Sample Incident

Some terms

- 3 entities involved in Internet domain name registration:
  - Registrants
    - Final client, the one who wishes to register the domain name
  - Registrars
    - Interface between registry and registrant, may provide extra services to the latter one.
  - Registries
    - Authoritative repository, responsible for all functional information required to resolve names registered in its TLDs

Registrant – Registrars – Registries Model



e.g. a sample company
Who wants to register,
Sampleco.com

e.g. .com domain registrars
Godaddy.com
Networksolutions.com

e.g. .com registry
Currently VeriSign

What is Domain Hijacking?

- To take practical control of a domain away from its rightful owner without using legal means.
- Also known as Domain Theft in some references.
- This may have severe consequences for the rightful domain owner and also for other parties.

Who are affected?

- Affects more parties than the rightful name holder.
- May affect:
  - Customers
  - Business Partners
  - Even parties wholly unrelated to the name holder

Damages caused by Domain Hijacking

- Registrant may lose its online identity with little recourse
- Exposes registrant to extortion by name speculators
- Disruption or malicious use of a registrant's Internet services
  - Denial and theft of electronic mail services
  - Unauthorized disclosure of information through phishing web sites
  - Traffic inspection (eavesdropping)
  - Damage to the registrant's reputation and brand through web site defacement

Motivations for Hijackers

- Money
  - Extortion
    - e.g. Hijacker to rightful Domain holder: Give me 20000$ dollars to return your domain.
  - Resell
    - E.g. Hijacker publish an advertisement on internet that a popular internet domain is for sale.
- Social reasons
  - Religious
  - Political
  - Revenge
  - Fun
  - …

How is it done?

- Different techniques
- It can be done by exploiting vulnerabilities in Registrant, Registrars or probably Registries.

How is it done?

- Method 1: Gaining access to the domain owner email address
  - The security of a domain name is highly related to the security of its owner's email address.
  - A domain owner's email address could be obtained in many cases by "Whois" service.

How is it done?

- Method 1(cont…)
  - Example: whois of WEB-JAPAN.ORG

Domain ID:D103667737-LROR
Domain Name:WEB-JAPAN.ORG
Created On:07-Jan-2004 07:47:16 UTC
Last Updated On:13-Apr-2009 21:15:57 UTC
Expiration Date:07-Jan-2011 07:47:16 UTC
Sponsoring Registrar:Melbourne IT, Ltd. dba Internet Names Worldwide (R52-LROR)
Registrant ID:D107344443424686
Registrant Name:The Ministry of Foreign Affairs of Japan
Registrant Street1:2-2-1,kasumigaseki
Registrant City:Chiyoda-ku
Registrant State/Province:Tokyo-to
Registrant Postal Code:100-8919
Registrant Country:JP
Registrant Phone:+81.355018454
Registrant Email: keiichi.nakahara@mofa.go.jp
Tech Email:keiichi.nakahara@mofa.go.jp
Name Server:NS6-TK02.OCN.AD.JP
Name Server:NS1.IWS.MOFA.GO.JP

How is it done?

- Method 1 sample scenario:
  - The domain owner email is somehow hacked.
  - The hijacker sends a ‘forget password’ to the registrar.
  - The registrar sends the administrative password of domain to the owner email.
  - Hijacker reads the password and gains control over administration panel of domain

How is it done?

- Method 2: Re-registering the Domain Name contained within the Admin Contact
  - WEB-JAPAN.ORG had an Admin Contact of keiichi.nakahara@mofa.go.jp
  - Hijacker waits until mofa.go.jp is expired and reregisters it. Sets up mofa.go.jp to have all emails to be forwarded to his gmail account, then requests a Transfer of Registrar on WEB-JAPAN.ORG

How is it done?

- Method 3: Impersonation using forged credentials
  - Misusing from a weak point in registrar procedures.
  - Hijackers use forged faxed requests or forged postal mail requests to modify registrant information.
  - In certain cases, official company letterhead is stolen or copied, modified or duplicated to abet the fraud.

How to prevent?

- Security measures for
  - Registrants
  - Registrars
  - Registries

Security Measures to Protect Domain Names

- Registrants
  - Keep domain name registration records accurate and current
  - Keep registrant account information (e.g., userid, passwd,…) private, secure, and recoverable
  - Choose a registrar with hours of operation that match the needs of the registrant
  - Use a *whois* Privacy Service

Security Measures to Protect Domain Names

- Registrants
  - Keep current and accurate registrar business and emergency contact information
  - Be familiar with and incorporate urgent restoration of domain name and DNS configuration procedures as part of business continuity policy and planning
  - Request that domain names be placed on Registrar-Lock.

Security Measures to Protect Domain Names

- Registrars and Registries
  - Using EPP
    - Extensible Provisioning Protocol
    - EPP "codes" or "keys" are also required in the transfer of generic top-level domain names between registrars
    - Gaining Registrar must provide Auth Code to the Registry when submitting Transfer order

Investigation

- Assume that an important domain name of one of your customers is hijacked
  - Hijacker has setup its own mail server to gain access to all incoming email addresses
- You want to know
  - How the hijacker hijacked the domain name.
  - Who is hijacker? (Legal investigation/Forensics)

Investigation

- How the hijacker hijacked the domain name?
  - Here we propose a simple procedure:
  - Find the answer to the following questions:
    - Step 1: Check if it is a case in which the domain has expired and another one has re-registered it
      - This is often can be done by checking the billing or administrative email address of domain and looking for possible warning expiration messages from registrar

- Step 2: Check if it is a case in which hijacker has gained access over administrative password of domain control panel
  - It may be done if the owner email account or his computer is hacked
    - Check domain owner computer for any kinds of Trojans, key loggers and spywares.
    - Is the owner email password changed?
    - Has the owner received suspicious emails from registrar?
- Step 3: Contact the registrar and inform them of the incident
  - Why the domain information has changed?
  - Does the registrar has received any request from anyone for domain transfer?

Investigation

- Who is the hijacker?
  - Not an easy answer for this question.
  - A possible solution is to find the new Admin/Owner email address?
    - Tracing hijacker email address
    - How to trace?
      - We propose a possible way in our case study.

How to recover?

- Standard recovery method: UDRP
  - UDRP: Uniform Domain Name Dispute Resolution Policy
  - Standard process for resolution of disputes regarding the registration of domain names.
  - Established by ICANN (Internet Corporation for Assigned Names and Numbers)
  - Currently applies to: all .biz, .com, .info, .name, .net, and .org top-level domains, and some country code top-level domains

How to recover?

- UDRP(Cont…)
  - The goal of the UDRP is to create a streamlined process for resolving such disputes.
  - It was envisioned that this process would be quicker and less expensive than a standard legal challenge.
  - A party dissatisfied by a UDRP decision may challenge the decision in court.
    - If a trademark holder loses a UDRP proceeding, it may still bring a lawsuit against the domain name registrant.

How to recover?

- Non-Standard methods
  - It depends mainly on registrars
  - Maybe faster
  - If the domain has not been transferred from one registrar to another
    - Contact the registrar and follow the required steps to recover the domains
  - If the domain has been transferred from one registrar to another
    - Take the issues to court

Sample Incident: religious domains

- Religious Domains: In Sep 2008, more than 300 domains, mostly Iranian religious domains, were hijacked.
  - sistani.org
  - alkhoei.net
  - alulbeyt.com
  - imamsadiq.org
  - and more...

Sample Incident: religious domains

- Registrar
  - Mydomain.com(A reseller of dotregister)
- Registrant
  - AalulbaytITC Company
- Complete Hijacking for sistani.org
  - One of the most popular clergy in Iran and Iraq
  - Domian was transfered from MyDomain.com to Godaddy.com

Sample Incident: religious domains

- Partial Hijacking for all other domains
  - Owner of domains was changed from AalulbaytITC to Hacker_XP(dreeming@yahoo.com)
- The defaced websites show some banners against clergies.
- Motivation for hackers
  - Socials reasons, not extortion
- Damage/Misuse
  - Web site defacement

Sample Incident: religious domains

- Steps
  - 1. The hijacker hacked the registrant email address
  - 2. Gain access to administrative password of domain panel in mydomain.com
  - 3. Change domain ownership for most of domains
  - 4. Transfer 1 or 2 domains to Godaddy.com

Sample Incident: religious domains

- Investigation
  - Step 1: Using Whois Database to find the email addresses of the new owner of the hijacked domains:
    - vre8@hotmail.com (for sistani.org)
      dreeming@yahoo.com (for all other hacked domains)

Sample Incident: religious domains

- Step 2: Tracing the IP addresses used by hijackers to access the above email addresses.
- Technique used for tracing IP Address
  - We Sent an email with an external image link to target mailboxes
  - When the hijacker opened the email a HTTP request was automatically sent to our server
  - Hijacker IP and his/her browser type was identified!!!

Sample Incident: religious domains

- Results of Investigation:
  - Time: Friday 19th of September 03:54:07 AM
    Email: dreeming@yahoo.com
    IP: 78.89.x.y
    Browser: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

  - Time: Friday 19th of September 2008 03:48:15 AM
    Email: torabora_1@yahoo.com
    IP: 78.89.x.y
    Browser: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Sample Incident: religious domains

- Some points
  - 78.89.??.?? maybe the hijacker real IP or the IP of a system which is controlled by him/her.
  - IP Whois: xxxxxxxx-TELECOM-xxx, xxxxxx
  - For further investigation of the case we needed an official organization in xxxxxx to cooperate with us
  - But unfortunately xxxxxx has no CERT to cooperate in investigation.

Conclusion

- The domain names are important assets need to be protected carefully.
- Domain hijacking incidents are common.
- The CSIRTs should increase the awareness regarding these incidents in their constituencies.
- They should be prepared to investigate and recover
- The cooperation of CSIRTs from several countries is necessary for a full investigation

References

- Religious Domains Incident Report, Amirkabir University of Technology APA Laboratory(CSIRT)
- Domain Name Hijacking: Incidents, Threats, Risks and Remedial Actions. http://www.icann.org/announcements/hijacking-report-12jul05.pdf
- R.Lao, B.Comm, Understanding Domain Hijacking, http://gold.domainmanager.com/ppt/DomainHijacking.ppt
- http://www.circleid.com/posts/help_domain_name_hijacked/, Brett Lewis, Jan 12, 2007.
- http://en.wikipedia.org/wiki/UDRP

Many thanks for your attendance