

# *Domain Name Hijacking*

Security and Stability Advisory Committee

Luxembourg

12 July 2005

# *Speakers*

- Steve Crocker, Chair
- Bruce Tonkin, CTO MelbourneIT
- Rodney Joffe, Chairman & CTO, UltraDNS
- Ram Mohan, CTO Afilias
  
- Dave Piscitello, SSAC Fellow

<http://www.icann.org/announcements/hijacking-report-12jul05.pdf>

# *Outline*

- Incidents
- Risks & threats associated with domain hijacking
- Vulnerabilities observed from domain hijackings
- Recovery mechanisms
- Security measures to protect domain names
- Findings
- Recommendations

# *Panix.com incident*

- Domain name transferred from rightful holder
- Name servers changed
- Impact
  - Website and subscriber email services disrupted
  - Major impact on business operations
  - Brand of longest operating NY metro ISP tarnished

# *Analysis of the Incident*

- Gaining registrar did not obtain approval from the registrant
  - reseller did not send authentication request to administrative contact address at PANIX
- Available mechanisms could have prevented incident
  - Domain name was not locked
  - Losing registrar did not elect to notify the registrant upon receiving the pending transfer notice from the registry
- EPP not used by .com at time of incident

# *Recovery Process Issues*

- Registrar transfer processes do not address situations where
  - An incident would occur on a weekend
  - Resolution would involve parties in different time zones
    - The gaining registrar attempted to confer with the losing registrar, the original registrant, the registry operator and the reseller to help authenticate the problem.
  - Emergency support staff rather than business contact numbers for all parties involved in an incident would be required.
  - Parties involved in incident response needed to share information they customarily keep private
    - The gaining registrar also needed to review event logs at both the registrar and its reseller.

# *Areas for Improvement*

- Registrars should
  - Make contact information for emergency support staff available to other registrars, resellers, and registry operators
  - Define a mechanism to resolve an urgent restoration of domain name registration information and DNS configuration
  - Improve registrant awareness of the availability and purpose of the Registrar-Lock
  - Consider improvements in the authentication and authorization mechanisms in protocols used for name transfers
- Losing registrar notifies a registrant upon receiving a pending transfer notice from the registry at its option
  - Objective of the transfer policy is to assure that registrars provide registrants with choice, notification and consent,
  - ICANN and registrars should try to determine whether registrants would generally favor mandatory notice

# Hush*mail* Incident

- Attacker
  - convinced 1st-tier support staff at registrar to modify the administrative email contact information in Hush's registration record
  - used the administrative contact email to submit a password reset request for the Hush account
  - accessed the Hush account, changed the password, and used the account to alter the DNS A record to the attacker's server
  - posted a defaced home page expressly designed to embarrass Hush and gain notoriety for the attacker.

Incident is labeled a "hijack" but did not involve a domain name transfer...

# *Analysis of Incident*

- Attacker
  - socially engineered a 1st-tier customer support agent who was relatively new to the company
  - was extremely familiar with registrar's customer service procedures and terminology
- Weekend incident: trend or coincidence?
- Vulnerability in registrar's customer service security measures contributed to the success of the attack
  - Has been rectified

# *Areas for Improvement*

- Identify situations where customer support should obtain supervisor approval before it changes registration records
- Do not use the same email for multiple purposes
  - One data object cannot be used as user account/identity, authentication and authorization
- Keep portions of registration record used for transfers and account access private (do not publish in Whois)
- Use > 1 form of contact for transfer and registration related notifications
- Obtain 24 x 7 emergency contact info from registrants
- Encourage registrants to lock domains and to make 2<sup>nd</sup> email address on different domain available for emergency contact

# *HZ incident*

- Registrant discovered registration information had been changed during a random Whois check
- Losing registrar claimed transfer was legitimate
  - Had email with FOA purportedly sent by registrant
  - Suggested but no firm evidence of email spoofing
- Losing registrar put onus on registrant to prove transfer was not authorized
  - Transfer dispute submitted after waiting period had expired
- Direct intervention with CEO of gaining registrar led to domain being returned to registrant
  - CEO based decision to restore domain on suspicious information in 80+ domains registered by same “hijacker”

# *Analysis of Incident*

- No changes made to DNS configuration
  - HZ.com services unaffected BUT
  - Registration changes may have continued undetected for indeterminate period
- Uncertain status
- Domain name was “frozen asset”

# *Recovery Process Issues*

- Incomplete audit and transaction records hampered investigation
  - Complete registration history not available
  - Inaccurate registration information
- Gaining registrar relied on an electronic process to obtain authorization
  - Transfer policy accepts consent from an individual or entity that has an email address matching the Transfer Contact email address as sufficient proof of identity
- Name holder of record did not receive a pending transfer notification for the domain name from the losing registrar

# *Areas for Improvement*

- Resellers should be able to provide a complete chronology of name holders
- Registrars should augment registration records to include dates of acquisition and a history of name holders
- Should the notification process be entirely dependent on (and satisfied by) email notification?
  - Should a 2<sup>nd</sup> contact or 2<sup>nd</sup> method of contact be provided or offered?

# *It's not just .com*

Domain	Outcome of Incident
Sex.com	Returned to Rightful owner 7 years later
ClubVibes.com	Recovered
iFly.com	Resold (not recovered)
Hackers.com	Resold (not recovered)
WiFi.com	Recovered
Babayiz.biz	Still under investigation
2e.com	Recovered (WIPO arbitration hearing)
Slsk.org	Lost
Ebay.de	Recovered

# *Outline*

- Incidents
- Risks & threats associated with domain hijacking
- Vulnerabilities observed from domain hijackings
- Recovery mechanisms
- Security measures to protect domain names
- Findings
- Recommendations

# *Risks and Threats (1)*

- To the registrant
  - Theft of domain name for resale, extortion
  - Tarnish of brand
  - Fraud, Identity Theft, Monetary Theft
  - Personal, Commercial and Political Espionage
  - Business Interruption
  - Collateral Damage
  - Loss through Litigation
  - Loss of customer/confidence, customer attrition

# *Risks and Threats (2)*

- To registries, registrars and resellers
  - Tarnish of brand
  - Loss through litigation
  - Loss of reseller business
  - Loss of accreditation and business operations
  - Loss of customer confidence
  - Customer attrition

# *Outline*

- Incidents
- Risks & threats associated with domain hijacking
- Vulnerabilities observed from domain hijackings
- Recovery mechanisms
- Security measures to protect domain names
- Findings
- Recommendations

# *Vulnerabilities Observed from Domain Hijackings*

- Potential for Registrant Fraud
  - Impersonation of rightful name holder
    - Use forged (physical) credentials (fax, stolen or copied company letterhead)
    - Social engineering
  - Hijacking the authorized email address of an administrative contact
- Potential for abuse/exploitation of registrar process
  - List follows

# *Vulnerable Aspects of Registrar Processes (1)*

- A formal registrant authentication process is circumvented through social engineering.
- A forged document is accepted physical proof of identity.
- Authentication credentials are disclosed to unauthorized 3rd parties by 1st-tier support staff, and no checks-and-balances safeguard against misuse of a 1st-tier support staff's ability to access and modify registrant credentials
- Gaining registrars use one (and often only one) form of contact, an email to administrative contact, to transmit the standard FOA used to notify registrant of a transfer request.

# *Vulnerable Aspects of Registrar Processes (2)*

- Registrars fail to make the availability and purpose of domain locking mechanisms known to registrants.
- The default setting of domain locks is not uniform across registrars.
- A registrar or reseller fails to follow authorization processes according to the transfer policy.
- A registrar, reseller or registrant fails to maintain accurate registrant information.
- Registrars do not have mechanisms to handle urgent restoration of a domain name.
- Registrars do not have sufficient contact information to assist in an urgent restoration of a name.

# *Vulnerable Aspects of Registrar Processes (3)*

- Registrars and resellers do not maintain a history of registration information
- Registrars do not publish best practices or set standards for auditing resellers
- A losing registrar is not required to notify the registrant upon receiving a pending transfer notice from the registry
- Registrars, registrants and resellers do not maintain alternate contact information to safeguard against circumstances where email service might not be operational in emergency situations

# *Outline*

- Incidents
- Risks & threats associated with domain hijacking
- Vulnerabilities observed from domain hijackings
- Recovery mechanisms
- Security measures to protect domain names
- Findings
- Recommendations

# *Recovery Mechanisms*

- UDRP
  - Available today, for abusive registrations or cybersquatting, particularly trademarked names
- TDRP
  - Available today for registrars to address disputes involving a transfer that has occurred
- Urgent Restoration of a Domain (proposed)
  - Emergency action channel
  - Accompanying policy
  - Public awareness campaign

# *Emergency Action Channel*

- 24 x 7 access to registrar technical support
- Staff is authorized to
  - Assess situation (legitimacy of claim)
  - Determine immediacy of need
  - Act! (restore registration information and DNS configuration)

# *Emergency Action Policy*

- Evaluation criteria
  - What information must a registrant provide to obtain immediate intervention?
  - Form the basis for action channel implementation
- Complements the TRDP
- Distinguishing characteristics
  - Immediacy of harm
  - Magnitude of harm
  - Escalating impact

# *Outline*

- Incidents
- Risks & threats associated with domain hijacking
- Vulnerabilities observed from domain hijackings
- Recovery mechanisms
- Security measures to protect domain names
- Findings
- Recommendations

# *Steps Registrants Can Take to Protect Domain Names (1)*

- Keep domain name registration records accurate and current
- Keep registrant account information private, secure, and recoverable
- Restrict registration account access to parties who “need to know”
- Choose a registrar with hours of operation that match the needs of the registrant
- Keep current and accurate registrar business and emergency contact information

# *Steps Registrants Can Take to Protect Domain Names (2)*

- Be familiar with and incorporate urgent restoration of domain name and DNS configuration procedures as part of business continuity policy and planning
- Investigate whether losses related to a registration or DNS configuration incident are covered by insurance policies.
- Request that domain names be placed on Registrar-Lock
- If your registrar uses EPP, use a unique EPP authInfo code for each domain name registered

# *Steps Registrants Can Take to Protect Domain Names (3)*

- Request that the losing registrar contact the registrant when a transfer request is received
  - Use a contact point separate from that used by the gaining registrar
- Routinely check the Whois service to check if a domain name is under Registrar-Lock
- Routinely check domain name information to ensure that no unauthorized changes have been made to the contact information
- Consult with your registrar to establish preferred authentication processes for removing a transfer lock or changing a domain name configuration

# *Steps Registrants Can Take to Protect Domain Names (4)*

- Choose a registrar who issues a transfer pending notification as its standard practice.
- Registrants seeking to further reduce risk should:
  - Choose a registrar who will notify the registrant using contact methods in addition to (and in parallel with) standard email notices.
  - Specify the number and kinds of contact methods that must be used for transfer and DNS configuration change notifications

# *Steps Registrars Can Take to Protect Domain Names (1)*

- Establish a more uniform implementation of EPP authInfo
  - Registrar-assigned authInfo codes must comply with transfer policy
  - Advise registrants of pros and cons of creating unique authInfo codes for their domain names
- Establish a uniform default setting of domain locks across registrar
- Investigate additional methods to improve accuracy of registrant records

# *Steps Registrars Can Take to Protect Domain Names (2)*

- Acquire emergency contact information for parties who can assist in responding to an urgent restoration of domain name
- Consider measures to improve authentication and authorization used in registrar business processes, especially:
  - change of delegation information,
  - change of contact details (credentials),
  - change of registrant (selling the name), and
  - change of registrar

# *Steps Registrars Can Take to Protect Domain Names (3)*

- Protect registrant information that can be used to facilitate fraud and impersonation, and theft of a domain name
  - Treat information that is used in registrant authentication processes as private
- Improve auditing of resellers' compliance with record keeping requirements
- Provide clear and readily accessible information to registrants regarding domain locking and domain name protection measures offered by registrars

# *Steps Registries Can Take to Protect Domain Names*

- Implement EPP authInfo
- Work with registrars to establish a more secure implementation of EPP authInfo codes
- Monitor use of EPP authInfo codes
- Work with registrars to define “best common practices” for auditing registration processing
- Work with registrars to improve authentication and authorization requirements for transfers and changes to SLD name servers within the TLD

# *Steps Resellers Can Take to Protect Domain Names*

- Review all relevant ICANN transfer policy documentation
- Establish a uniform default setting of domain locks
- Investigate additional methods to improve accuracy of registrant records
- Acquire emergency contact information for parties who can assist in responding to an urgent restoration of domain name
- Consider measures to improve authentication and authorization used in reseller business processes
- Provide clear and readily accessible information to registrants

## *Steps ICANN take to minimize the negative impacts of transfers on the registrant*

- Consider developing a set of graduated penalties for registrars that fail to comply with the transfer policy
- Publish additional consumer information that explains the domain transfers policy and processes, and identifies the areas of risk for a registrant

# *Outline*

- Incidents
- Risks & threats associated with domain hijacking
- Vulnerabilities observed from domain hijackings
- Recovery mechanisms
- Security measures to protect domain names
- Findings
- Recommendations

# *Findings 1-3*

- **Finding (1)** Failures by registrars and resellers to adhere to the transfer policy have contributed to hijacking incidents and thefts of domain names.
- **Finding (2)** Registrant identity verification used in a number of registrar business processes is not sufficient to detect and prevent fraud, misrepresentation, and impersonation of registrants
- **Finding (3)** Consistent use of available mechanisms (Registrar-Lock, EPP authInfo, and notification of a pending transfer issued to a registrant by a losing registrar) can prevent some hijacking incidents.

# *Findings 4-5*

- **Finding (4)** ICANN Policy on Transfer of Registrations between Registrars specifies that “consent from an individual or entity that has an email address matching the Transfer Contact email address” is an acceptable form of identity. Transfer Contact email addresses are often accessible via the Whois service and have been used to impersonate registrants.
- **Finding (5)** Publishing registrant email addresses and contact information contributes to domain name hijacking and registrant impersonation. Hijacking incidents described in this report illustrate how attackers target a domain by gathering contact information using Whois services and by registering expired domains used by administrative contacts.

# *Findings 6-7*

- **Finding (6)** Accuracy of registration records and Whois information are critical to the transfer process. The ICANN Whois Data Reminder Policy requires that registrars annually request registrants to update Whois data, but registrars have no obligation to take any action except to notify registrants. Registrants who allow registration records to become stale appear to be more vulnerable to attacks.
- **Finding (7)** ICANN and registries have business relationships with registrars, but no relationship with resellers (service providers). Resellers, however, may operate with the equivalent of a registrar's privileges when registering domain names. Recent hijacking incidents raise concerns with respect to resellers. The current situation suggests that resellers are effectively "invisible" to ICANN and registries and are not distinguishable from registrants. The responsibility of assuring that policies are enforced by resellers (and held accountable if they are not) is entirely the burden of the registrar.

# *Findings 8-10*

- **Finding (8)** ICANN requires that registrars maintain records of domain name transactions. It does not appear that all registrars are working closely enough with their resellers to implement this requirement.
- **Finding (9)** The Inter-Registrar Transfer Policy incorporates formal dispute mechanisms. These were not designed to prevent incidents requiring immediate and coordinated technical assistance across registrars. Specifically, there are no provisions to resolve an urgent restoration of domain name registration information and DNS configuration.
- **Finding (10)** Changes to transfer processes introduced with the implementation of the ICANN Inter-Registrar Transfer Policy have not been the cause of any known attacks against domain names. There is no evidence to support reverting to the earlier policy.

# *Outline*

- Incidents
- Risks & threats associated with domain hijacking
- Vulnerabilities observed from domain hijackings
- Recovery mechanisms
- Security measures to protect domain names
- Findings
- Recommendations

# *Recommendations 1-2*

1. Registries should ensure that **Registrar-Lock and EPP authInfo are implemented.**

Registries should confirm registrars **do not use the same EPP authInfo** code for all domains.

2. Provide resellers and registrants with **Best Common Practices** that describe **appropriate use and assignment of EPP authInfo** codes...

# *Recommendations 3-4*

3. (Today) a losing registrar notifies a registrant upon receiving a pending transfer notice from the registry **at its option**.
4. Registrars should make contact information for emergency support staff available.

Registrars should provide **an emergency action channel**.

# *Recommendations 5-6*

5. Identify evaluation criteria a registrant must provide to obtain immediate intervention
6. Conduct a public awareness campaign to identify the criteria and the procedures registrants must follow to request intervention and obtain immediate restoration of a domain name and DNS configuration.

# *Recommendations 7-8*

7. Improve accuracy/integrity of registrant records.

Emergency contact information from registrants

8. Improve awareness of domain name hijacking and registrant impersonation and fraud.

Encourage use of Registrar-Lock and authInfo

Supplement with monitoring and maintenance of contact and authentication information.

# *Recommendations 9-10*

9. ICANN should investigate whether stronger and more publicly visible enforcement mechanisms are needed.
10. ICANN should consider whether to strengthen the identity verification requirements in electronic correspondence.