Domain Name Hijacking: Incidents, Threats, Risks and Remediation

Document 007 Version 1

Executive Summary

This report by the Security and Stability Advisory Committee (SSAC) describes incidents where domain names were "hijacked". Domain hijacking refers to the wrongful taking of control of a domain name from the rightful name holder. The common use of the term encompasses a number of attacks and incidents. Incidents representative of common forms of attacks are discussed and analyzed in the report. The Committee then presents its findings and recommendations.

As the report illustrates, domain hijacking can have a lasting and material impact on a registrant. The registrant may lose an established online identity and be exposed to extortion by name speculators. Domain hijacking can disrupt or severely impact the business and operations of a registrant, including (but not limited to) denial and theft of electronic mail services, unauthorized disclosure of information through phishing web sites and traffic inspection (eavesdropping), and damage to the registrant's reputation and brand through web site defacement. The report further illustrates how incidents often affect more parties than the rightful name holder: customers, business partners, consumers of services provided by the name holder, and even parties wholly unrelated to the name holder are often "collateral damage" to hijacking incidents.

The Committee finds that domain name hijacking incidents are commonly the result of flaws in registration and related processes, failure to comply with the transfer policy, and poor administration of domain names by registrars, resellers, and registrants.

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.

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.

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 are held accountable if they are not) is entirely the burden of the registrar.

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.

On the basis of these findings, the Committee makes the following recommendations:

Recommendation (1): Registries should ensure that Registrar-Lock and EPP authInfo are implemented according to specification. In particular, registries should confirm that registrars comply with the transfer policy and do not use the same EPP authInfo code for all domains they register.

Recommendation (2): Registries and registrars should provide resellers and registrants with Best Common Practices that describe appropriate use and assignment of EPP authInfo codes and risks of misuse when the uniqueness property of this domain name password is not preserved.

Recommendation (3): Under the current transfer policy, a losing registrar notifies a registrant upon receiving a pending transfer notice from the registry at its option.

Registrars should investigate whether making this notice a mandatory action would reduce hijacking incidences.

Recommendation (4): Registrars should make contact information for emergency support staff available to other registrars, agents of registrars (resellers), and registry operators. Specifically, registrars should provide an emergency action channel. The purpose of this channel is to provide 24 x 7 access to registrar technical support

staff that are authorized to assess an emergency situation, establish the magnitude and immediacy of harm, and take measures to restore registration records and DNS configuration in circumstances which merit such intervention.

Recommendation (5): Registrars should identify evaluation criteria a registrant must provide to obtain immediate intervention and restoration of domain name registration information and DNS configuration. Registrars should define emergency procedures and policy based on these criteria. This policy would complement the Transfer Dispute Resolution Policy (TDRP) and must not undermine or conflict with those policies.

Recommendation (6): ICANN, the registries, and the registrars should 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.

Recommendation (7): Registrars should investigate additional methods to improve accuracy and integrity of registrant records. More frequent or alternate communications might assist registrants in keeping their information up to date. Registrars should also acquire emergency contact information from registrants for technical staff who are authorized and able to assist in responding to an urgent restoration of domain name incident.

Recommendation (8): Registrars should improve registrant awareness of the threats of domain name hijacking and registrant impersonation and fraud, and emphasize the need for registrants to keep registration information accurate. Registrars should also inform registrants of the availability and purpose of the Registrar-Lock, and encourage its use. Registrars should further inform registrants of the purpose of authorization mechanisms (EPP authInfo), and should develop recommended practices for registrants to protect their domains, including routine monitoring of domain name status, and timely and accurate maintenance of contact and authentication information.

Recommendation (9): ICANN should investigate whether stronger and more publicly visible enforcement mechanisms are needed to deal with registrars that fail to comply with the transfer policy, and to hold registrars accountable for the actions of their resellers.

Recommendation (10): ICANN should consider whether to strengthen the identity verification requirements in electronic correspondence to be commensurate with the verification used when the correspondence is by mail or in person.
