ICANN

Dear Registrar Contact,

We would like to bring to your attention the security risks associated with an operational practice related to the use of sacrificial name servers in the Extensible Provisioning Protocol (EPP) as described in the paper titled “Risky BIZness: Risks Derived from Registrar Name Management”.

Quoting from the paper, the issue arises “*in particular situations wherein [a] domain has subordinate host objects (typically representing nameservers) referenced by other domains, the constraints dictated by EPP do not allow the domain to be removed — even by the registrar of the domain. Over the years, registrars have developed an operational workaround for this limitation, in which the registrars rename host objects subordinate to the domain within the EPP system to enable removal of the domain. The host objects thus renamed are given an entirely new domain name that typically falls under the authority of a different top-level domain (TLD) operated by a different registry.*”

For example, “*the nameserver ns2.example.com, on expiry of the domain example.com, might be renamed within the registry to {randomstring}.biz. As a result, any domain name in the .com TLD that had delegated its nameservice to ns2.example.com would find that nameserver silently replaced with {randomstring}.biz.*”

They also found out that ”*in most cases this renaming is entirely mechanical and no attempt is made to register the new domain name (or, for that matter, to validate that the new name is not already registered). As a result, any party assuming control of {randomstring}.biz is subsequently able to control name resolution for all of the domains that had previously used ns2.example.com for name service. Perhaps more importantly, as a result of the renaming, a simple re-registration of example.com will not fix the issue.*”

They discovered that over a period of nine years (what their data set covered), more than half a million names were exposed to the risk of hijacking by this practice. Of those, they concluded that almost a third were hijacked. The authors characterized these numbers as a lower bound given the limitations of their methodology.

You can watch their presentation at the recent IETF at https://youtu.be/9Fxe8b5iwd8?t=1050

We encourage you to review your operational procedures to verify whether your registrar is following the highlighted practice and if so, to take measures to mitigate the security risks described in the paper. Potential mitigation measures include: 1) removing the name servers of domain names whose hostname is under a name that is already or about to be removed; or 2) the use of a dedicated “sink domain name” under your control. You may also want to monitor hostnames you use as name servers that are not under your control, in case the sponsoring registrar of the parent domain name follows the risky practice, so you can react appropriately.

If you have any questions, please contact ICANN Global Support.

Regards,

Technical Services Team
Global Domains and Strategy
Internet Corporation for Assigned Names and Numbers