Tuesday, July 25, 2023
From: "k claffy"

Dear Theresa,

The SSAC has chartered its Registrar NS Management (RNM) Work Party with considering domain resolution hijacking risks that are unintended consequences of operational practices between domain registrars and registries, and options for prevention and remediation. In particular, the work party is exploring the risks that emerge from the expiration of domains that other domains rely on for authoritative DNS name service. It has become a common operational practice to rename such nameservers outside a registry's delegated namespace -- frequently to unregistered domains in a separate TLD. Over the last nine years these practices have exposed over 500k domains to resolution hijacking risk. This behavior has been observed in both unrestricted TLDs (including .com and .net) as well as restricted TLDs (such as .edu and .gov). Multiple parties have actively exploited this weakness, hijacking control over 163K domains.

This work party is investigating options for detection, remediation, and preventing new exposure. The work party will analyze the effectiveness of possible solutions, and base any recommendations on these analyses. We are also exploring possibilities and requirements for formal documentation and monitoring of this observed phenomenon beyond what is currently known. In order for us to make evidence-based recommendations we would like to see additional analyses of the scope of the behavior at present, and historically over time.

Specifically, we request ICANN org technical staff:

. Conduct an analysis that identifies across all gTLDs the numbers of: sacrificial nameservers, exposed domains, hijacked nameservers, and hijacked domains.

. This analysis should include host objects that are not in the DNS zone files but are in the registry database so as to accurately capture all instances of this phenomenon.

. The analysis should be aggregated at the registrar level and
the registry level.

. The analysis should be reported by month going back to at
least April 2011.

We appreciate that it may take a little bit of time to consider and respond to this request. We will be happy to interact informally to clarify this request or reformulate it if need be. In the meantime, we kindly request that you provide us with an estimate of the possible completion time for this analysis.

Thank you and kind regards,

kc, on behalf of the SSAC Registrar Name Management Work Party