SSAC
ICANN Security and Stability Advisory Committee

June 10, 2009

SAC041: Recommendation to prohibit use of redirection and synthesized responses by new TLDs

SSAC advises ICANN that new TLDs, including both new gTLDs and new ccTLDs, should not use DNS redirection and synthesized DNS responses. We recommend ICANN take all available steps with appropriate entities to prohibit such use. We also recommend that ICANN communicate our concerns with other parties who might be able to act independently of ICANN to ensure that the dangers inherent in redirection and synthesized responses not only in TLDs but at subordinate levels of the DNS are understood, that the consequences are considered carefully, and that measures to assure the integrity of error as well as name resolution is preserved.

The redirection and synthesizing of DNS responses by TLDs poses a clear and significant danger to the security and stability of the domain name system. The consequences of synthesized DNS responses range from erosion of trust relationships to the creation of new opportunities for malicious attacks, without the ability of the affected party(ies) to mitigate these problems.

The Security and Stability Advisory Committee has studied the matter of redirection and synthesized responses (also known as *wildcarding*) at the top level of the DNS on four occasions since 2004. A synopsis of each study is listed below.

In 2007, security researchers began investigating the unintended consequences of a growing *error resolution* market, which attempts to analyze and monetize “name error” DNS responses by introducing modification or redirection at various points along a response path the answer to a particular DNS response may take. In addition to the security and stability issues earlier forms of redirection introduced, these new practices exposed domain registrants to new attacks. In particular, security researchers (notably, Dan Kaminsky) were able to demonstrate that vulnerabilities in web applications running at redirection sites could be exploited to the harm of domain registrants. In response to this new threat landscape, SSAC published SAC032, *Preliminary Report on DNS Response Modification*, in January 2008. The report examined error resolution and redirection practices in use at the time and called attention to numerous security and stability concerns:

> “By the very nature of the DNS, any third party who provides an iterative resolver that participates in the resolution process is a potential man in the

> middle and has the ability to modify messages it receives from an authoritative name server before forwarding these to a client."
>
> "DNS response modifications can affect applications other than web and in particular can disrupt email, Internet telephony, and other Internet services."
>
> "DNS response modifications can create unpredictable responses (nominally a stability issue, but in the worst case possibly resulting in a denial of service attack)."
>
> "Any application or management activity that relies on NXDomain (name error) responses for correct operation or intervention will no longer work for all labels within the domain that are redirected." (In the context of TLD redirection, organizations that seek to protect brands from infringement may not be able to use the same automation, in the same manner, if that automation relies on name error answers from TLD name server operators).

In November 2006, following a proposed new service request by Tralliance, the Registry Services Technical Evaluation Panel was convened to study this request and published a report entitled *Report on Internet Security and Stability Implications of the Tralliance Corporation search.travel Wildcard Proposal*. In the report, RSTEP concludes that the wildcard service "does create a reasonable risk of a meaningful adverse effect on security and stability." SSAC supported RSTEP's report and published a complementary advisory, SAC 015, entitled *Why Top Level Domains Should Not Use Wildcard Resource Records*. An additional purpose of SSAC's explanatory work was to summarize the problems redirection at the TLD level creates for a broader audience. The substance of the recommendation remained the same:

> "TLDs should refrain from using services that make use of wildcard services and synthesized DNS reponses."

In SAC006, Redirection in the COM and NET Domains, SSAC made certain findings that illustrate the adverse effects redirection at the TLD level can have. In particular, SSAC determined that redirection

> "… disturbed a set of existing services that had been functioning satisfactorily. Names that were mistyped, had lapsed, had been registered but not delegated, or had never been registered in DNS were resolved as if they existed. As a consequence, certain e-mail systems, spam filters and other services failed resulting in direct and indirect costs to third parties, either in the form of increased network charges for some classes of users, a reduction in performance, or the creation of work required to compensate for the consequent failure."

At that time, SSAC recommended that

> “Synthesized responses should not be introduced into top-level domains (TLDs) or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries over which the operator may have little control or influence.”

SSAC notes that the original contract between ICANN and the .MUSEUM TLD included wildcarding but this concession was removed when the contract was revised.

SSAC reiterates its position that synthesized DNS responses at the TLD level (and subordinate levels) is a destabilizing practice. It also creates opportunities for DNS abuse that can be easily avoided and should be prohibited at TLD registries. We urge ICANN, and the global DNS community to find appropriate mechanisms to ban this practice at the TLD level.

Acknowledgements

The committee wishes to thank the following members for their time, contributions, and review during SSAC's study of this matter:

Jaap Akkerhuis
Lyman Chapin
Steve Crocker
Jeremy Hitchcock
Ram Mohan
Dave Piscitello
Ray Plzak
Paul Vixie