

Tracking DNSSEC Errors Over the Holiday Period

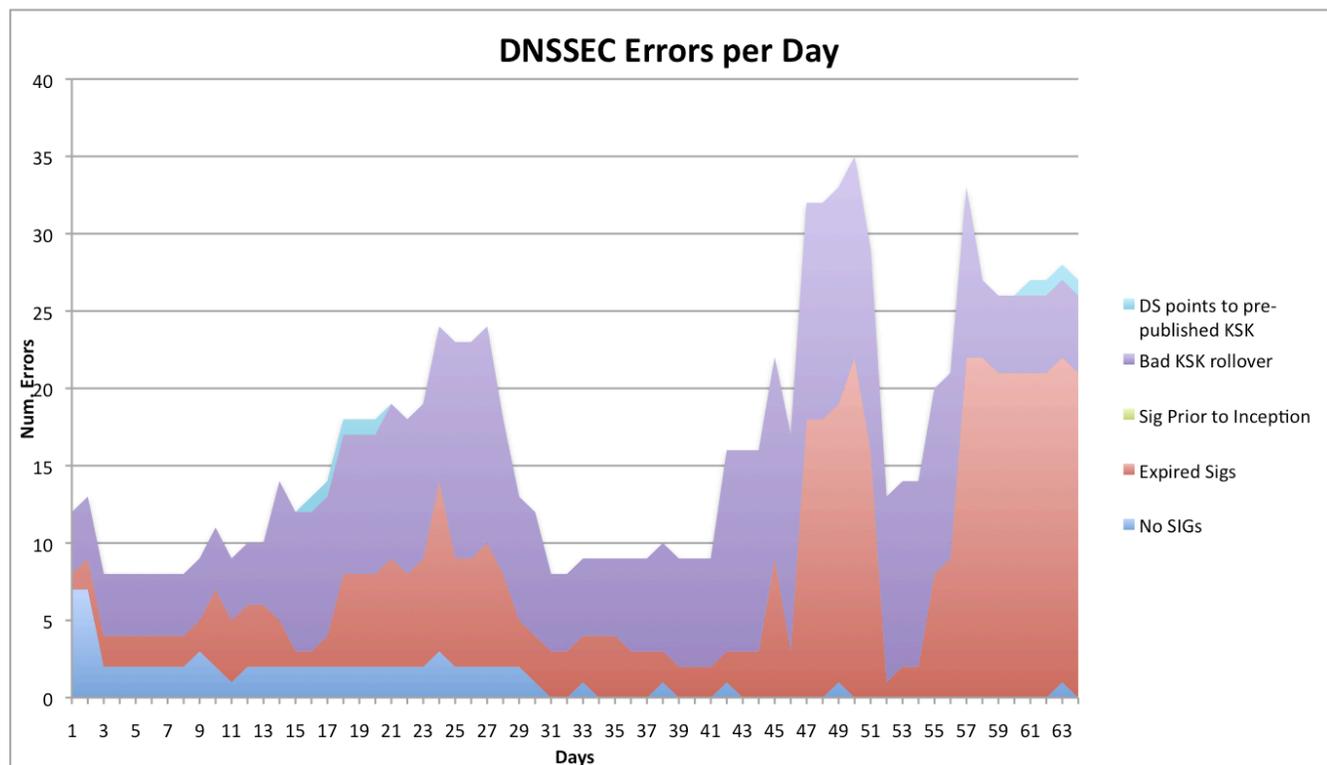
Scott Rose, NIST

scott.rose@nist.gov

produced 1/5/2012

NIST has been tracking the DNSSEC related errors seen every day from the vantage point of a typical Internet user – i.e. a validator with just the DNS Root Zone key installed as a trust anchor. The tool uses BIND as a validating resolver, so both UDP with TCP fallback is used. Below is the chart of errors seen by type from Nov 2nd 2011 until Jan 4th 2012, a time period covering the Thanksgiving, winter holidays and New Years.

Previous to the start of this, the daily total of all errors seen in the previous 3 months averaged around 12-17 errors on any given day (including weekends). Considering the number of signed zones in .gov (about 830 growing to 880+ zones), this error rate is tolerable, if not ideal. However, the growth in errors seen during periods of staff leave indicates that DNS operations in some agencies need to be improved.



In the above chart, the error types tracked are:

- No Sigs: The zone in question has a DS RR in the .gov TLD and possible DNSKEY RR's are seen in the zone, but no signatures are seen in responses.
- Expired Sigs: The zone has DNSKEY RRs in the zone and valid DS RR in .gov, but the signatures have expired (RRSIG expiration date is in the past).
- Sigs Prior to Inception: The zone has DNSKEY RRs in the zone and valid DS RR in .gov, but

the signatures have an inception date in the future.

- Bad KSK Rollover: It appears that the zone has rolled its KSK, but has failed to update its DS RR in .gov.
- DS points to pre-published DNSKEY: The zone has DNSKEY RR's, but the DS RR in .gov contains a hash of a DNSKEY that is present, but not used to generate signatures.

As shown in the table above, there are spikes of errors seen during the holiday weeks (days 19-24 for Thanksgiving and days 47 on for Christmas and New Years (Dec 17th onward to Jan 4th as many may have took leave starting Dec 19, the week before Christmas). There are dips in the errors as IT staff come back from leave and fix issues, but many remain over the long holiday week between Christmas and New Years. This was noticed last year as well (2010-2011) but was not as pronounced due to the smaller number of DNSSEC signed zones in .gov at the time compared to this year.

With more validation being done, the zones that are in an error state on any given day are effectively “gone” from the Internet. These could be errors, or they could be part of an attack against a client, so the DNSSEC specification calls for these error responses to be rejected by the client as an attack.

Recommendations

This trend in errors over time periods when IT staff are likely on leave or lightly staffed indicates a need for better automation of DNS and DNSSEC operations or backup IT staff for DNS operations when primary staff are on leave. That would likely solve many of the “Sig Expired” type errors.

Better automation won't necessarily fix the “Bad KSK Rollover” type errors, as there needs to be action by both the zone operator and the .gov TLD (through the dotgov.gov web portal for example). The actions on how to do a KSK rollover in a secure manner are detailed in NIST SP 800-81r1 and RFC 4641 on DNSSE operations. In summary, a zone must add the new KSK, but sign with both the new and old KSK until the new DS (containing the hash of the new KSK) appears in the .gov TLD. Only after waiting for the new DS to appear (and wait the TTL of the DS RR) is it safe to remove the old, expired KSK. Administrators should also then remove the old, expired DS RR from .gov, which often requires a second visit to the dotgov.gov portal to remove the DS RR for the expired KSK.

References

R. Chandramouli and S. Rose “Secure Domain Name System (DNS) Deployment Guide” NIST SP 800-81r1 April 2010. <http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf>

O. Kolkman and R. Gieben. “DNSSEC Operational Practices”, RFC 4641. September 2006
<http://datatracker.ietf.org/doc/rfc4641/>