Details

ICANN (Internet Corporation for Assigned Names and Numbers) Blog

Author: Matt Larson, VP of Research, Office of Chief Technology Officer

18 Jul 2018

Minimal User Impact Expected From Root Zone (Root Zone) Key Signing Key (KSK) Rollover

The ICANN (Internet Corporation for Assigned Names and Numbers) organization believes that an update of the Domain Name (Domain Name) System Security (Security – Security, Stability and Resiliency (SSR)) Extensions (DNSSEC (DNS Security Extensions)) trust anchor for the global Domain Name (Domain Name) System (DNS (Domain Name System)) on 11 October 2018 will affect only a very small number of DNS (Domain Name System) users. The decision to roll the root zone Key Signing Key (KSK) is being made after a significant outreach effort and careful consideration of all available data.

Since the DNS (Domain Name System) root zone was originally signed in 2010, the DNSSEC (DNS Security Extensions) Practice and Policy Statement[1] has set the expectation that the root zone KSK will change. Fortunately, most validating resolvers that observe a new root zone KSK should be able to configure it as a new trust anchor automatically using "Automated Updates of DNS (Domain Name System) Security (Security – Security, Stability and Resiliency (SSR)) (DNSSEC (DNS Security Extensions)) Trust Anchors," defined in RFC5011[2]. A resolver operator can also update their trust anchor configuration manually if they have become aware that the root KSK is changing based on ICANN (Internet Corporation for Assigned Names and Numbers)'s various outreach efforts.

There is no standardized or deterministic way to actively measure that a validating resolver has the correct set of trust anchors configured. The best method currently available is "Signaling Trust Anchor Knowledge in DNS (Domain Name System) Security (Security – Security, Stability and Resiliency

(SSR)) Extensions" (documented in RFC (Request for Comments) 8145[3]) that was published in April 2017. In that protocol, validators emit a DNS (Domain Name System) query that contains the DNSKEY key IDs of configured trust anchors in the query name. These queries can be passively observed in traffic at the root servers. In September 2017, there were a handful of resolvers using this protocol and the announcements of trust anchors showed a higher percentage of misconfigured trust anchors than initially anticipated. However, the signal observed at the time was not well understood and, as a result, the ICANN (Internet Corporation for Assigned Names and Numbers) org decided to postpone the root zone KSK roll to better understand the signal with the help of the technical community.

Further research by the ICANN (Internet Corporation for Assigned Names and Numbers) org's Office of the CTO (OCTO) team and others revealed concerns with the quality of the RFC (Request for Comments) 8145 data. For example, a DNS (Domain Name System) query reporting trust anchor information that is sent to a forwarder is treated the same as any other query and will be sent to a root server regardless if the forwarder is validating or not. In one case, a popular DNS (Domain Name System) resolver implementation signaled the trust anchor even though the resolver was not configured to validate and thus would not have the new trust anchor. This implementation decision was reversed in a subsequent release of the software. In another case, a well-known DNS (Domain Name System) resolver library signaled the trust anchor but did not have a method to automatically update its trust anchor configuration. As a result, a single deployment of a popular single-user VPN implementation using that DNS (Domain Name System) resolver library would emit the old trust anchor signal from different source addresses over time. Wes Hardaker at the University of Southern California Information Sciences Institute discovered this behavior and the vendor using the library was informed and updated their software. This change has significantly reduced the number of sources reporting the old trust anchor.[4]

However, the RFC (Request for Comments) 8145 data reports only resolvers; it does not provide an indication of the number of end users dependent upon those resolvers. To understand the size of the population of users behind validating resolvers, the Regional Internet Registry for the Asia Pacific region (APNIC (Asia-Pacific Network Information Center)) used a measurement system that utilizes Google's advertising network to query the DNS (Domain Name System). Analyzing the intersection of ICANN (Internet Corporation for Assigned Names and Numbers)'s trust anchor signaling sources with their own resolver sources and then extrapolating, APNIC (Asia-Pacific Network Information Center) calculated that only 0.05 percent of Internet users would be negatively affected by the root KSK roll.[5]

Looking forward, the ICANN (Internet Corporation for Assigned Names and Numbers) org will soon reach out to the 1,000 Internet Service Providers (ISPs) with the most active resolver traffic that suggests DNSSEC (DNS Security Extensions) validation has been enabled in order to ensure they aware that the root KSK roll will occur on 11 October 2018. Those ISPs will also be surveyed

on their preparation plans for the rollover, which may cause those resolver operators to become more aware of the KSK rollover.

Since the first announcement of the development of plans to roll the trust anchor in 2015, the ICANN (Internet Corporation for Assigned Names and Numbers) org has maintained an outreach campaign that has (to date) included nearly 100 speaking engagements at international, regional, and national conferences, and more than 150 news stories in the technical press. The ICANN (Internet Corporation for Assigned Names and Numbers) org has also published nine blog articles related to the trust anchor rollover and continues to reach out to the ISPs that have validating resolvers in their networks but which, from RFC (Request for Comments) 8145 data, do not appear to have the new trust anchor configured.

As a result of these efforts and the data we have been able to collect, the ICANN (Internet Corporation for Assigned Names and Numbers) org has increased confidence that the root KSK rollover planned for 11 October 2018 will have the potential to affect only a tiny fraction of DNS (Domain Name System) users.

---

[1] https://www.iana.org/dnssec/icann-dps.txt (https://www.iana.org/dnssec/icann-dps.txt)

[2] https://datatracker.ietf.org/doc/rfc5011/ (https://datatracker.ietf.org/doc/rfc5011/)

[3] https://datatracker.ietf.org/doc/rfc8145/ (https://datatracker.ietf.org/doc/rfc8145/)

[4] http://root-trust-anchor-reports.research.icann.org/ (http://root-trust-anchor-reports.research.icann.org/)

[5] http://www.potaroo.net/ispcol/2018-04/ksk.pdf (http://www.potaroo.net/ispcol/2018-04/ksk.pdf) [PDF, 184 KB]

Comments

Log in to Comment (/users/sign_in) or Sign Up (/users/sign_up)