Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets

- Domain Generation Algorithms (DGAs)
  - are tools which ‘input’ a specific date and time, and ‘output’ a domain name for that specific time.
  - Some of the largest and most dangerous botnets - such as Conficker and Avalanche - have been controlled via the use of Domain Generation Algorithms (DGAs)

- Law Enforcement (LE) action vs Botnets
  - Low Frequency / High Impact events
  - each domain only needs to be seized for a short duration at the specific date/time specified by the DGA.

- Improving upon DGA referrals was identified by PSWG/RySG as “low hanging fruit” / attainable goal
  - Recommends voluntary & non-binding Best Practices
  - Streamlining for an **EVERGREEN** solution
    - One action / referral by LE to Ry’s, and by Ry’s to ICANN, enabling **EVERGREEN** action going forward for that DGA.
      - Avoiding wherever possible the need to keep "coming back to the well"
  - Thanks to ICANN for willingness their feedback and guidance on engaging the “Expedited Registry Security Request” mechanism

QUESTIONS