Questions & Answers on Domain Name System Attacks

(Ref: ICANN Announcement of 22 February 2019)

Q: Why is ICANN issuing statements now?
A: After ICANN became aware of the attacks, through reports from media and security professionals, it was important to take steps to ensure the ICANN community and the public at large was also made aware of the situation. This is in keeping with our mission to ensure the security and stability of the Domain Name System (DNS).

Q: What kind of attack is it?
A: Public reports indicate that there is a pattern of multifaceted attacks utilizing different methodologies. Some of the attacks target the DNS. They use unauthorized changes to the delegation structure of domain names, replacing the addresses of certain servers with the addresses of machines controlled by the attackers. This particular type of attack, which targets the DNS, only works when Domain Name System Security Extensions (DNSSEC) are not in use.

Q: Who is behind these attacks?
A: There are conflicting reports about who is behind the attacks, and it is often difficult to specifically determine the actual party sponsoring such attacks.

Q: Is law enforcement investigating the attacks?
A: Public reports indicate law enforcement and national security bodies in multiple countries are investigating the attacks. Civil society (DNS engineers, cybersecurity experts, and others) are also actively working to identify the types of attacks used. They are also helping affected organizations harden their systems.

Q: Has ICANN been compromised?
A: We have no indication that ICANN systems were compromised. We have completed a systems review out of an abundance of caution.

Q: Have any root servers been compromised?
A: There are no indications that any of the DNS root servers have been compromised. ICANN has contacted the Root Server System Advisory Committee (RSSAC) to request that it consult with the root server operators to confirm there are no indications of compromise. To date, no root server operator has notified us that a compromise was detected.

Q: How widespread is the risk? How many domain names are unsecured?
A: Part of the attack leveraged passwords that had been compromised. It is impossible to know how many other passwords might be compromised. Thus, we again encourage all parties in the DNS ecosystem to use strong passwords, to rotate them often, not re-use passwords across multiple sites, and to use multi-factor authentication whenever possible.

Q: Are the attacks still continuing? When did they start? When did they stop?
A: While we are unaware of ongoing attacks, we believe that there is an ongoing risk. We encourage all organizations to improve their online security, including implementing

Domain Name System Security Extensions (DNSSEC), if they have not already done so. They should also ensure that their credentials for domain name management are strong and review their systems for signs of compromise, tampering, etc. Published reports suggest the current set of attacks started as far back as 2017.

Q: Does ICANN recommend any specific actions?
A: Yes, on 15 February 2019, ICANN offered the following checklist, though this does not include all the measures that could be implemented to assure full security:

- Ensure all system security patches have been reviewed and have been applied
- Review log files for unauthorized access to systems, especially administrator access
- Review internal controls over administrator ("root") access
- Verify integrity of every DNS record, and the change history of those records
- Enforce sufficient password complexity, especially length of password
- Ensure that passwords are not shared with other users
- Ensure that passwords are never stored or transmitted in clear text
- Enforce regular and periodic password changes
- Enforce a password lockout policy
- Ensure that DNS zone records are DNSSEC signed and your DNS resolvers are performing DNSSEC validation
- Ideally ensure multi-factor authentication is enabled to all systems, especially for administrator access
- Ideally ensure your email domain has a DMARC policy with SPF and/or DKIM and that you enforce such policies provided by other domains on your email system

Q: Will implementation of DNSSEC protect end users?
A: Yes. Implementing DNSSEC will protect users from specific types of attacks. Some of the systems that were used to mount the attacks used domain names that were protected by DNSSEC, and the owners of those zones have confirmed that their use of DNSSEC helped mitigate the attacks.