ICANN

Dear Registrar contact,

In the recent DNS OARC 40 workshop a group of researchers presented about a cyber attack that is being observed. The researchers claim that the top 20 vendors with 70% market share are vulnerable. Briefly, the attack unfolds when DNS records normally used to point to content delivery networks or other web hosting providers are left undeleted after the service is no longer used by the registrant, combined with other factors in the web hosting service.

For registrars offering DNS and/or web hosting services directly or through other service providers, we thought it would be wise to alert you to the attack. ICANN strongly encourages you to take the necessary measures in your DNS and web hosting services to mitigate this risk, such as avoiding leaving "dangling DNS records", strengthening domain ownership validation processes, and ensuring your web hosting service is not vulnerable in any of the various ways described in slide 39 and table 3 in the paper.

You can find their slides at https://indico.dns-oarc.net/event/46/contributions/982/attachments/933/1740/oarc40_li_dareshark.pdf

You can find their paper athttps://www.researchgate.net/publication/368471344_Detecting_and_Measuring_Security_Risks_of_Hosting-Based_Dangling_Domains

If you have any questions, please contact ICANN Global Support.

Regards,

Technical Services Team
Global Domains and Strategy
Internet Corporation for Assigned Names and Numbers