Exposing Hundreds of Rogue VPN Domains Potentially Connected to the NSA

Posted on October 1, 2021

WhoisXML API DNS Threat Researcher Dancho Danchev identified domain intelligence related to several bogus free VPN service providers. Those bogus entities could seemingly be traced back to the National Security Agency (NSA) as part of an effort to monitor the online activities of suspicious Iran-based users.

Dancho Danchev looked into the domain infrastructure of these cited NSA-initiated VPN services and prepared lists of assets that could help the security community monitor the campaign. Among the critical information included in the report are:

- 20+ domain names involved in the identified NSA's fake VPN service campaign
- 20+ registrant email addresses believed to be involved in the campaign
- 260+ connected domain names

Monitoring these Internet properties can help security researchers and threat intelligence analysts with domain asset attribution and further studies. Get access to 300+ domain clues related to this potentially rogue VPN service campaign and learn how to uncover more.

Download the report now.