DNS on FIre

Published: 2019-11-07 · Archived: 2026-04-02 11:17:58 UTC

This presentation by Warren Mercer and Paul Rascagneres (Cisco Talos) was delivered at VB2019 in London, UK. Cisco Talos identified malicious actors targeting the DNS protocol successfully for the past several years. In this presentation, we will present two threat actors we have been tracking. The first one developed a piece of malware, named DNSpionage, targeting several government agencies in the Middle East, as well as an airline. During the research process for DNSpionage, we also discovered an effort to redirect DNSs from the targets and discovered some registered SSL certificates for them. We identified multiple countries targeted by this redirection. On 22 January 2019, the US DHS published a directive concerning this attack vector. We will present the timeline for these events and their technical details. The second actor is behind the campaign we named 'Sea Turtle'. This actor is more advanced and more aggressive than the previous one. They do not hesitate to directly target registrars and one registry. The talk will present the two actors and the methodology used to target the victims. https://www.virusbulletin.com/confere...
