WhoisXMLAPI

Analyzing “Brian Krebs” Typosquatting Domains to Spread Malware

Posted on May 11, 2021

Brian Krebs[1], an American journalist and investigative reporter, is best known for his coverage of cybercrime & cybersecurity news—notably through his blog KrebsOnSecurity.com.

Krebs’s work has made his blog a popular source for cybersecurity professionals and news reporters. Including his name in domain names could serve as a good lure to reel victims into malware traps.

WhoisXML API Threat Researcher Dancho Danchev uncovered two command-and-control (C&C) server domains that could easily be mistaken to be associated with Krebs. Using those as jump-off points for cybersecurity investigations led to the discovery of other connected web properties that could pose risks to networks.

Download the report now to get access to the investigation’s initial findings.

- [1] https://en.wikipedia.org/wiki/Brian_Krebs