

ABSTRACT

A botnet domain name family detecting method, an apparatus, a device, and a computer-readable storage medium. Said method comprises: acquiring suspicious domain
5 names; constructing a domain name spatiotemporal association graph on the basis of associations between various suspicious domain names in different dimensions; taking each suspicious domain name as a node in the domain name spatiotemporal association graph, two domain names having at least one association forming an edge therebetween, and the association between the two domain names serving as an attribute value of the edge; and
10 according to determination indexes of a compactness degree between various nodes in graph calculation, determining closely associated domain names in the domain name spatiotemporal association graph, and taking a set of the corresponding domain names as a botnet domain name family. The present application shows the associations between domain names in various different dimensions uniformly in the form of an association graph, and has a stronger detection
15 capability. Moreover, the invention is able to detect a botnet domain name family quickly, and is widely applicable.