CND Assignment 2 Write-up

Rajat Vij

I created my domain generation algorithm after reading through <https://johannesbader.ch> J. Bader’s blog. I used the program that was already provided and modified it to have properties of the Karken’s two DGA version 2 and Symmi.

Kraken (also known as *Oderoor* or *Bobax*) was once a large, if not the largest, botnet. It was primarily used to send spam messages. Kraken features a Domain Generation Algorithm (DGA) which appeared in July 2007 and was first mentioned in 2008. This makes it one of the first ever widely used DGA.[Quoted from the blog]

Virus scanners label the sample as *Symmi*, other names for the same or similar malware family are *MewsSpy* and *Graftor.*[Quoted from the blog]

J. Bader has reverse engineered multiple DGA observed in various malwares, viruses, botnets and trojan’s. I chose these as I found them both somewhat understandable (unfortunately I was unable to understand the reverse engineering process in all of his blog posts) and found that Karken was using date and seed sets which we can choose whereas Symmi was making the generated Domain somewhat spell-able giving generated domain a genuine feel. Both use PRNG algorithms to add complexity to the generated domains (I went with the PRNG algorithm that was used in Kraken’s version 2 although I tried using simple Random() of python to achieve the same result but I am not sure why that made the program a bit slow, maybe I implemented the function in an incorrect way.)

I have included comment’s in my code to make it more understandable and I was able to explain the algorithm there in a better way so please refer to the code to further understand the constructed algorithm.