Reflexión Actividad 3.4

Para problemas del tipo como el planteado en la situación problema, el uso de estructuras como un BST puede implicar una eficiencia mayor a la hora de ejecutar el programa, pues al ser de tipo no lineal y estar ordenada de manera que las búsquedas se pueden reducir en tiempo, gracias a que están organizados en base al tamaño del contenido del nodo,

Así, por ejemplo, si se tiene un árbol con una gran cantidad de números, y se busca uno de gran tamaño, con el primer paso que toma para la búsqueda basta para notar la posible eficiencia, ya que probablemente el número va a estar a la derecha de la raíz, por lo que nos evitamos recorrer toda la parte izquierda del árbol, al seguir este tipo de recorrido, se puede decir que el movimiento por un BST es de complejidad logarítmica.

En cuanto al problema de detectar si una red está infectada, un método que se me viene a la mente, con el uso de un BST, sería dirigirse a los sitios con más visitas en la red, analizando si los URL son regulares o irregulares, o simplemente detectando si la cantidad de visitas sobrepasa al promedio, con respecto al mismo o a las demás.

Una recomendación clave que nos da AVG, es detectar, si es posible la raíz de la botnet, para así detener a las demás, aunque depende del tipo de botnet, pero al tener el registro de los sitios visitados, los usuarios, la cantidad de visitas, las tendencias de visita, entre muchos más datos, puede ser posible ir rastreando con el paso inverso de los días, el momento y el responsable de iniciar la botnet en tu red, tomando acciones como las que se nos han planteado en las actividades.

Referencias:

AVG (2018) *What is a botnet and how can you protect your computer*. Recuperado de: https://www.avg.com/en/signal/what-is-botnet