# LA GUERRA DE LOS BOTS: ATAQUES CIBERMÉTICOS.

Andrea Yela González - A01025250
Joshua Ruben Amaya Camilo - A01025258

## BOTMASTER

La computadora **cmpxaw7lxdyhb63ocpgb.xxx** fue usada para descargar la infección hacía **kevin.reto (172.21.65.54)**

También se observa otro dominio anómalo **bofgd2egwezcd8n3kplv.org**

## ¿QUÉ SUCEDIÓ?

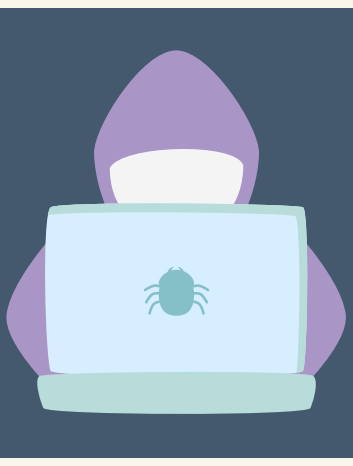
kevin.reto visitó una página llamada foodnetwork.com, la cual lo re dirige al Sitio anómalo. Haciendo que kevin.reto se convierta en el sub servidor de comando y control.

Empieza un **ping sweep** al momento de la infección el **17-08-2020.** Recorriendo las IP Internas del 0-254 encontrando **computadoras vulnerables** que esperan instrucciones.

El siguiente día Kevin recibe instrucciones de atacar; le manda la instrucción a las otras computadoras internas y estas comienzan el ataque.

### TIPO DE ATAQUE

- Fue un ataque **DDoS hacía iris.gov,** saturando la página.



## GRAFOS & ÁRBOLES

Estas estructuras nos ayudaron para encontrar el ataque, el sitio anómalo, las cantidades de conexión hacia ese sitio y saber la estrategia utilizada.

## ESTRUCTURAS LINEALES Y LISTAS

A pesar de dar información sobre la base de datos, estas estructuras no ayudan de forma precisa determinar la información del ataque.

**36894 registros de archivo**

**Red Interna 172.21.65**

## ¿QUÉ HARÍAMOS DIFERENTE?

Desde un principio construir el árbol para determinar la conexión, además de crear códigos eficientes que no necesiten tanto espacio en memoria.