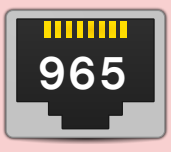
Karla Valeria Mondragón Rosas Ximena Sánchez Padilla

SITUACIÓN PROBLEMA

LA GUERRA DE LOS BOTS: ATAQUES CIBERNÉTICOS

El dominio anómalo **4FTJZR4G5U8GAWCSNJV1.COM** utilizaba el puerto

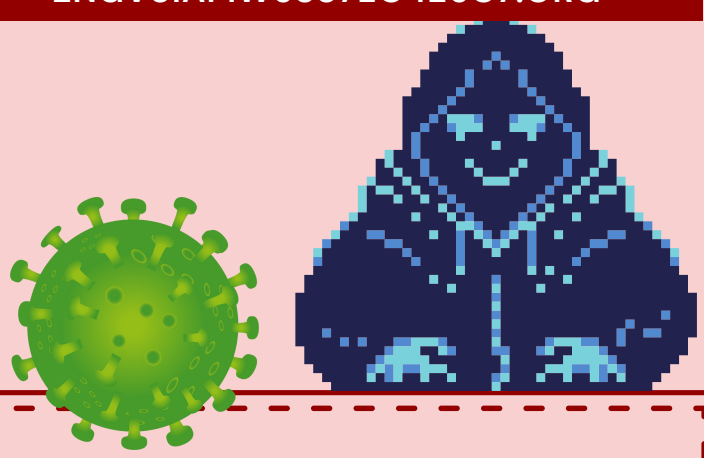


que se utiliza como servidor de comunicaciones IP y establece un código para implementarlo a clientes de forma remota (malware). Se utilizó para descargar la infección y controlar las computadoras infectadas.

BOTMASTER

DOMINIO

2NGV8IAMW6S87EO4Z6C7.ORG



LA COMPUTADORA INFECTADA REALIZA UN PING SWEEP PARA DETERMINAR LOS EQUIPOS ACTIVOS EN EL DOMINIO DE RETO.COM E INFECTAR A ESTOS EQUIPOS

Paciente 0

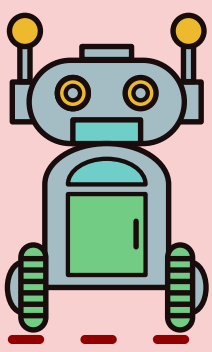
El equipo de

con ip 172.22.55.15, fue el equipo infectado el **14 de agosto**

ATAQUE DDOS A

18 de agosto 2020

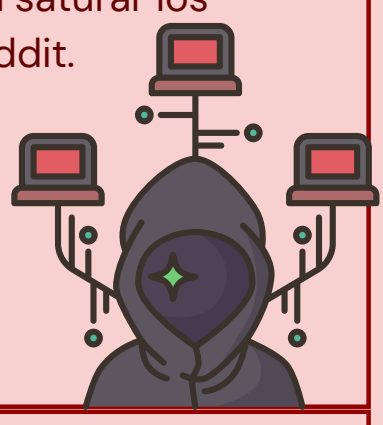
Las computadoras infectadas se conectan a mary.reto.com y esperan instrucciones.



TEORÍA

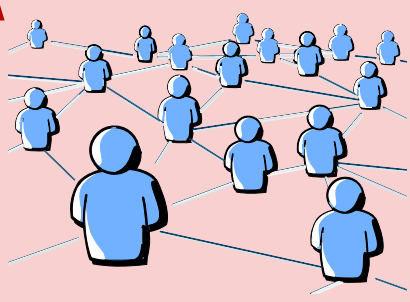
Por medio de un mail malicioso, el equipo de mary.reto.com se infecta.

- El 14 de agosto a las 12:00:29 hrs el equipo de mary.reto.com se comunica por primera y única al botmaster.
- Mary se conecta por primera vez al C&C.
- Mary.reto.com infecta a otros equipos del dominio reto.com
- Las computadoras infectadas esperan instrucciones.
- Ataque DDoS donde todas las computadoras del dominio reto.com buscan saturar los servidores de reddit.



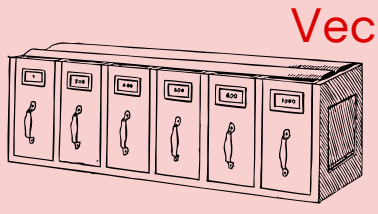
ESTRUCTURA MÁS ÚTIL

Diccionarios y grafos



ESTRUCTURA MENOS ÚTIL

Vectores



¿CÓMO MEJORAR?

- Diseñar un algoritmo que revise el tráfico en tiempo real para detectar actividades sospechosas
- Utilizar algoritmos de Big Data que permitan el procesamiento de grandes cantidades de información
- Representación visual de estas estructuras