Ataque Cibernético

ANDREÍNA SANÁNEZ, A01024927
ANA PAULA KATSUDA, A01025303

Se analizaron las conexiones de las computadoras pertenecientes a la compañía "reto.com" durante 11 días. Los descubrimientos fueron los siguientes:

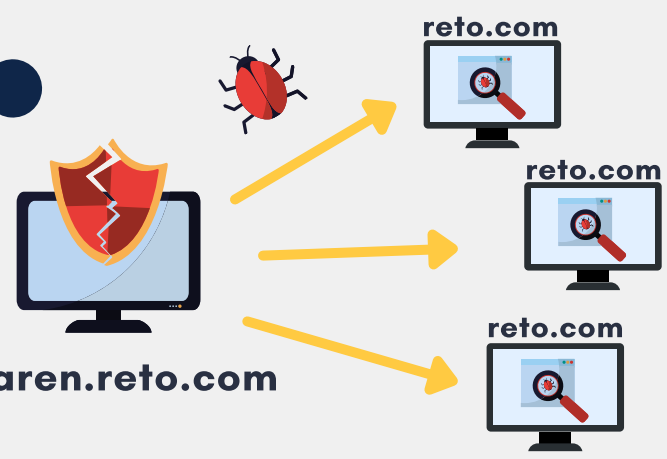
Se encuentran dos dominios anómalos: **j73fzlugbhbhy3k8jgmv.com** que solo tiene una interacción y **p7necksgkbynlvmgenv5.org** que permanece activo durante los demás días.

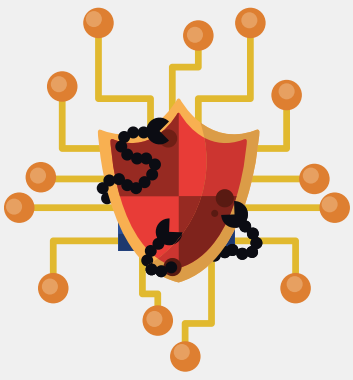
karen.reto.com

1° computadora infectada

El 17-08-20 "**karen.reto.com**" es la primera computadora interna en interactuar con los sitios anómalos.

El mismo día "karen.reto.com" se conecta con **cada una** de las computadoras internas y de esa manera, distribuye la infección.



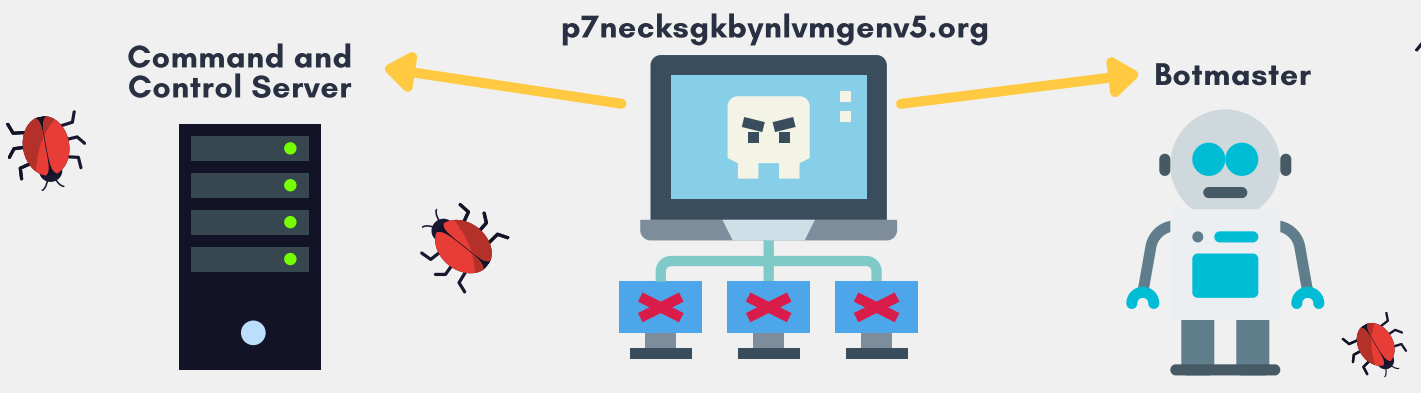


A partir de la infección, **todos los días** las computadoras de la compañía se conectan con **p7necksgkbynlvmgenv5.org**

El 18-08-20 se detecta un alto número de conexiones al sitio web **wiktionary.org** provenientes de la compañía.

Se identifica un ataque **DDoS** hacia **wiktionary.com** con una duración de un día.

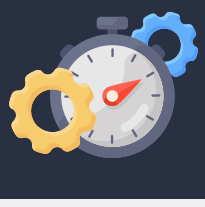
p7necksgkbynlvmgenv5.org es el **command and control server** y el **botmaster** del ataque



Estructuras

La más útil: grafo y diccionario

La menos útil: array



Lo que cambiaríamos: reto 4, fue muy ineficiente dado que utilizamos la clase ConexionesComputadora que implicaba muchos recursos