**Reporte Reto 5**

En esta entrega se nos encargo crear dos grafos en donde pudiéramos ver las conexiones que ocurrieron. El primer grafo nos enseña las conexiones que se realizaron entre las computadoras de la red interna, mientras que el segundo grafo nos enseña las conexiones que se realizaron de las computadoras de la red interna hacia diferentes sitios web. Esta información fue filtrada por día, es decir dependiendo de la fecha podemos ver las conexiones que se realizaron.

Con estos grafos podemos como el ataque fue realizado. Podemos observar de donde provino y hacia donde estaba dirigido. Esto se hizo viendo las conexiones que la computadora interna de la cual teníamos sospecha hizo cada día. Resulto que esta computadora (carol.reto.com) se conecto a 31 otras computadoras de la red el día que sucedió el ataque. Sabemos que este día comenzó el ataque ya que fue la primera y única conexión que hubo entre nuestro primer sitio malicioso (gncbrmxpm138gzbscrle.ru) y una computadora de la red interna (carol.reto.com). Después que se realizó esta conexión, ese día y todos los días subsecuentes las computadoras de la red interna se conectan a el segundo sitio malicioso (in6u9mmzf2o5dwr8o43l.ru).

Esto nos deja con una clara imagen de como las computadoras de nuestra red fueron infectadas. Lo que sucedió fue que por alguna razón el 14-8-2020 la computadora denominada “carol.reto.com” se conectó al sitio “gncbrmxpm138gzbscrle.ru” lo cual probablemente causo que se descargara algún tipo de código malicioso. Este realizo un ping sweep el cual es una técnica para saber cuantas computadoras existen en nuestra red interna. Ya con las computadoras de la red interna identificadas el código malicioso se reprodujo mandándose el mismo a través de un puerto TCP a las demás computadoras de la red.

Ya con todas las computadoras de la red interna infectadas con el código malicioso, cada una se conectó a “in6u9mmzf2o5dwr8o43l.ru” que presentimos que es un servidor de comando y control. Con toda esta información podemos estar seguros de que nuestras computadoras ahora son parte de una red de bots enorme que se conecta diario a el servidor de comando y control esperando que un Botmaster (El cual es una persona que tiene el control de todas las computadoras dentro de la red de bots) les de una instrucción.

Curiosamente dentro de las fechas del registro podemos ver la red de bots en acción. Como ya habíamos identificado en un reporte pasado, el día 18-8-20 existía un numero anormal de conexiones que sucedieron hacia el sitio “twitter.com”. Checando nuestros grafos podemos observar que ese mismo día todas las computadoras de nuestra red interna se conectaron al sitio. Con esta información asumimos que se esta realizando un ataque “DDoS” el cual es un ataque de denegación de servicio. Este tipo de ataque tiene como objetivo inhabilitar un servidor para que no puede recibir las conexiones de sus usuarios.

**Referencias**

Rouse, M. (Sep 2005). Ping Sweep (ICMP Sweep). [Sitio Web]. Recuperado de <https://searchnetworking.techtarget.com/definition/ping-sweep-ICMP-sweep>

Leonardo. (s.f) ¿Que es un BotMaster? [Sitio Web]. Recuperado de <https://botifica.com/blog/que-es-un-botmaster/>

Surveillance Self-Defense. (s.f). Servidor de Comando y Control. [Sitio Web]. Recuperado de <https://ssd.eff.org/es/glossary/servidor-de-control-y-comando>

OVHcloud. (s.f). ¿Qué es un Anti-DDoS? [Sitio Web]. Recuperado de <https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml>