Instituto Tecnológico de Estudios Superiores de Monterrey
Campus Santa Fe

Profa. Vicente Cubells

Programación de estructuras de datos y algoritmos fundamentales.

Jorge Pérez, A01023859
Luis Fernández, A01023675

23 de noviembre de 2020

Como parte de la situación problema se nos pidió investigar en qué consisten los términos de ping sweep, DDoS, servidor de comando y control y botmaster a continuación, sus definiciones.

Ping sweep: Es un método para atacar un rango de direcciones IP que se asigna a 'hosts' en vivo para encontrar vulnerabilidades. GTI. (S.D.)

DDoS: Un ataque de denegación de servicio distribuido, también conocido como DDoS tiene como finalidad incapacitar algún servicio o sistema remoto para imposibilitar su uso por distintos usuarios. Esto se puede lograr de dos maneras. La primera es a través de la saturación del ancho de banda. El cual imposibilita la conexión de terceros. La segunda se logra consumiendo todos los recuros (en procesamiento) del servidor. OVHCloud. (S. D.)

Servidor de comando y control: Un servidor de comando y control consiste en una estructura de múltiples servidores y diversos protocolos para controlar malwares y recibir información extraída de redes infectadas. Trend Mircro.(S.D.)

Botmaster: Un botmaster es la persona encargada de operar los servidores de comando y control en el contexto de ejecución de procesos remotos en botnets. DDoSPedia. (S.D.)

Reflexiones:

Luis Fernández:

Jorge Pérez:

Creo que en la situación problema, podría haber un ataque del tipo servidor de comando y control, ya que como se menciona previamente, es un uso común el disfrazar el tráfico como enviós de correo electrónico. Esta es una característica que notamos en el entregable pasado, donde se detectó un tráfico anormal a las direcciones de correo.

Suponendo que los atcantes de la situación problema ocupan una botnet para infectar a las personas de la red, considero que el sititio que el sitio fuente de la infección es "8w2v29sbezi1btcj4txw.com" o "euo5ychfvuhangmtt8uh.com".

Además de esto, estuve pensando en las implicaciones necesarias para detecertar este tráfico anomálo y simplemente no procesarlo, ya que es una de las maneras más frecuentes de evitar los ataques DDoS. Esto lo relacióné inmediatamente con la situación problema, ya que las estructuras de datos nos permitieron identificar de

manera rápida y eficiente el tráfico no legítimo, así como sus posibles fuentes de origen. Finalmente, creo que una buena continuación de esta práctica sería identificar el botmaster, en caso de que sea posible.

Referencias:

GTI. (S.D.). Ping Sweep. Sitio Web. Recuperado de: http://www.tugurium.com/gti/termino.php?Tr=ping%20sweep

OVHCloud. (S. D.) ¿Qué es un ataque DDoS? Sitio Web. Recuperado de: https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml

Trend Mircro.(S.D.) Command and Control [C&C] Server. Sitio Web. Recuperado de: https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server

DDoSPedia. (S.D.) Botmaster. Sitio Web. Recuperado de: https://security.radware.com/ddos-knowledge-center/ddospedia/botmaster/