Analysis of Botnet behavior as a distributed system

María José Erquiaga[1,3], Sebastián García[2], and Carlos García Garino[1]

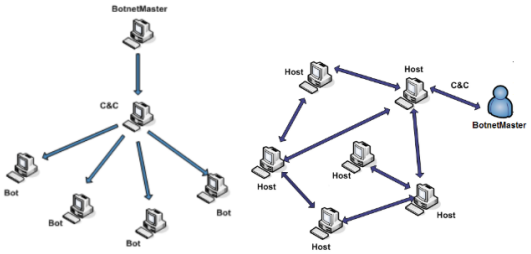
[1]ITIC, FIng, FCEN, Universidad Nacional de Cuyo , Mendoza, Argentina , merquiaga@uncu.edu.ar
[2]CTU University , Praga, República Checa , sebastian.garcia@agents.fel.cvut.cz
[3]ITIC, FIng, FCEN, Universidad Nacional de Cuyo , Mendoza, Argentina , cgarcia@itu.uncu.edu.ar

Abstract

El crecimiento vertiginoso de nuevas tecnologías, trae aparejado el crecimiento de aplicaciones maliciosas. Estas aplicaciones hacen uso de los recursos de los dispositivos infectados para realizar actividades ilícitas, enviar mails de forma masiva (spam) o minar para obtener criptomonedas. Para minar, se requiere grandes capacidades de cómputo Las *botnets* pueden ser consideradas como un tipo de de aplicación de computación distribuída. La palabra botnet significa red de robots. Es un tipo de malware, instalado en una computadora que ha sido infectada, con la habilidad de auto propagarse hacia otras máquinas. Todas las computadoras infectadas conforman la "red de bots", o botnet. Este tipo de malware utiliza los recursos de la computadora infectad (CPU, RAM, ancho de banda), para comunicarse con su Botnet Master, que es quien le da órdenes. El presente trabajo es un estado del arte, se analiza el comportamiento de las botnets como aplicaciones de computación distribuída. Se considera el comportamiento a nivel de consumo de recursos de los dispositivos que son infectados por el malware, en particular los miners.

1 Introducción

La definición de sistemas distribuídos por Tanembaum et al [8] es la siguiente: *Un sistema distribuido es una colección de computadoras autónomas enlazadas por una red y equipadas con un sistema de software distribuido. Este software permite que los computadores coordinen sus actividades y compartan recursos.* Esta definición hace referencia a dos aspectos importantes: los componentes autónomos, es decir, dispositivos que forman parte de este sistema, y la capacidad de las aplicaciones que funcionan en estos sistemas para trabajar de manera colaborativa. Concretamente, los sistemas distribuídos consisten de dispositivos con capacidad de cómputo interconectados entre sí, los cuales funcionan de forma autónoma y que trabajan juntos, aparentando ser un único sistema coherente.



(a) Centralized Botnet (b) Decentralized Botnet

Figure 1: Arquitecturas de Botnets

Por otro lado, las botnets, son un tipo de aplicación maliciosa, que pueden consideradas como un tipo de de aplicación de Computación Distribuida. La palabra botnet significa red de robots y consiste de un tipo de malware que es instalado en una computadora que ha sido infectada y tiene la habilidad de auto propagarse hacia otras máquinas. De esta manera, todas las computadoras infectadas conforman la "red de bots", o botnet. Posteriormente, cada botnet utiliza los recursos de la computadora infectada (CPU, RAM, memoria, ancho de banda), para comunicarse con su Botnet Master, que es quien le dará las órdenes. La arquitectura de este tipo de malware (botnet) puede ser centralizada o descentralizada. Éstas arquitecturas se pueden observar en la figura 1, donde (a) es la arquitectura centralizada y (b) descentralizada.

La computación distribuida permite resolver prob-

In: Proceedings of the IV School of Systems and Networks (SSN 2018), Valdivia, Chile, October 29-31, 2018. Published at http://ceur-ws.org

lemas de computación masiva mediante el uso de un gran número de computadoras que conforman una red distribuida. Esto significa, que existen varios dispositivos con gran capacidad computacional, conectados entre sí, resolviendo problemas que tienen la característica de ser intensivos en uso de CPU. Las botnets son un tipo de malware que hacen uso de esta tecnología para realizar actividades ilícias. Las botnets hacen uso de los recursos de un dispositivo infectado con el fin de obtener beneficios para el botnet master, uno de los usos es la obtención de bitcoins. Los bitcoins son una criptomoneda que ha cobrado mucho auge en los últimos años [5] [7]. Para generar esta moneda, se realizan operaciones computacionales que requieren de mucha capacidad de cómputo. Por este motivo, para realizar sus operaciones se requieren de varios nodos (dispositivos computacionales) que forman parte de la red Bitcoin. Los nodos bitcoin almacenan una lista de todas las transacciones en una cadena de bloques que se denominan mineros. Luego, todos los mineros de la red, compiten para ser los primeros en encontrar una solución a un problema criptográfico mediante algoritmos que para ser ejecutados y obtener una solución. Para lograr este objetivo, realizan operaciones que demandan de grandes capacidades de cómputo.

Para detectar las aplicaciones maliciosas se realizan análisis de su comportamiento, se buscan características y se genera un modelo de comportamiento, varios autores han aplicado esta técnica [6, 4, 2, 3]. Para poder obtener resultados reales, se ejecutan aplicaciones maliciosas en un laboratorio. Esto se realiza teniendo en cuenta una metodología de trabajo, para capturar los datos necesarios para el análisis. En trabajos anteriores, se han ejecutado aplicaciones maliciosas y capturado el tráfico de red, esto ha permitido obtener datos para analizar el comportamiento del malware y así comprender su funcionamiento. [1].

La hipótesis detrás de estos sistemas (Botnets), es que existe un conjunto de operaciones inherentes a cada aplicación/software que opera en la red. Este conjunto de operaciones es similar a una aplicación HPC, ya que se utilizan los recursos de la PC local (computadora infectada), y luego hay comunicación entre otros bots o entre el bot y el master. Luego, a partir de la observación y análisis de este comportamiento es posible afirmar que las botnets son un tipo de aplicación de HPC. Los datos a analizar son: (i) comportamiento del malware, de forma individual (ii) comportamiento de la botnet, es decir de la red de bots (iii) análisis del consumo de CPU, memoria y ancho de banda.

El proceso para este estudio consiste de tres etapas. En una primera etapa se realiza un análisis del malware (tipo de malware, cómo se comporta, qué pasos sigue tras la ejecución, etc). Se seleccionarán 3 variantes de malware de tipo miner, y se ejecutarán por lo menos 3 muestras diferentes de cada uno. En una segunda etapa se ejecuta el malware en un entorno de laboratorio (un servidor con varias máquinas virtuales para infectar), y se monitorea el consumo de CPU, memoria y ancho de banda. Posteriormente, se agregan otros dispositivos móviles (smartphones, tablets, cámaras IP, raspberries, etc) y se monitorea el comportamiento. El objetivo de esta etapa es obtener una red híbrida y analizar el uso de los recursos en dos escenarios posibles: con y sin la capa de virtualización.

En el presente trabajo se presenta una descripción de los malware de tipo miner (por ejemplo bitcoin miner o litecoin miner). Se seleccionarán 3 variantes de malware de tipo miner, y se ejecutarán por lo menos 3 muestras diferentes de cada uno. Se seleccionarán teniendo en cuenta qué tan reciente es el malware y la cantidad de dispositivos afectados por el malware. Este tipo de malware será utilizado para realizar los experimentos y analizar en comportamiento. Este malware fue seleccionado por sus características similares a las aplicaciones HPC (para los sistemas operativos windows, linux, android, otros). La similaridad se debe al uso excesivo de memoria RAM y de procesamiento que requieren los miners [1].

References

[1] M. J. Erquiaga, S. García, and C. García Garino. "Observer effect: How Intercepting HTTPS traffic forces malware to change their behavior". In: *Computer Science – CACIC 2017.* (2017).

[2] S García. "Modelling the Network behaviour of Malware to Block Malicious Patterns. The Stratosphere Project: a Behavioural IPS." In: *Proceedings of Virus Bulletin Conference 2015. Virus Bulletin Conference 2015, Prague* (2015).

[3] S. Garcia et al. "An Empirical Comparison of Botnet". In: *Detection Methods. Computers Security* (2014).

[4] Firdausi I., Lim C., and Erwin A.and Nugroho A. S. "Analysis of Machine learning Techniques Used in Behavior-Based Malware Detection". In: *Second International Conference on Advances in Computing, Control, and Telecommunication Technologies* (2010).

[5] A. Kundu, C. Kundu, and K. Budhraja. "Security Analytics of Network Flow Data of IoT and Mobile Devices". In: *CoRR* (2017). URL: `http://arxiv.org/abs/1704.03049`.

[1] Cryptocurrency Mining Craze Going for Data Centers: https://www.bitdefender.com/files/News/CaseStudies/study/196/Bitdefender-Whitepaper-Cryptocurrency-Mining-Craze-Going-for-Data-Centers-2018.pdf

[6] Erquiaga M.J., Catania C., and Garcia Garino C. "An analysis of network traffic characteristics for Botnet detection". In: *CACIC, WSI* (2012).

[7] Böhme R. et al. "Bitcoin: Economics, Technology, and Governance." In: *Journal of Economic Perspectives* (2015).

[8] Tanenbaum A. S. *Sistemas Distribuídos: principios y paradigmas*. Pearson Educación, 2007.