*[[1]](#footnote-1) Abstract— As there’s not platform for the DDoS attack securing, nor low cost stress test performing, platforms, nor botnets with IoT devices knowledge; have been found the needing of creating open, accessible and free knowledge about heterogeneous botnets and its application in a controlled environment, so in that way make awareness about the IoT devices security and their applicability on distributed systems for performing DDoS attacks without the user consent. Thanks to its low cost, have been found the possibility of using these devices for the coordinated attacks on a heterogeneous botnet.*

UPBotnet: Un proyecto de software libre para botnets heterogéneas en IoT.

UPBotnet

Alberto Manuel García Grimaldos, Oswaldo Andrés Angarita León: Universidad Pontificia Bolivariana Bucaramanga, alberto.garcia.2016@upb.edu.co, 3012102423.

*On this paper you will find an open source project development licensed under GNU/GPLv3 for the different characteristics machines (computers, IoT devices, smartphones, micro-controlled boards…) interconnexion on a high availability botnet, using MQTT protocol with interchangeable master nodes and dynamic charge assignation; destined to get type services denegation attacks.*

*It’s desired to complement the project progress, which is on production phase, for continuing adding devices with the informatics security open source community.*

*Keywords— Botmet, mqtt, IoT, micro-controlled boards, DDoS, high availability, GNU/GPLv3*

*Resumen— Dado que no existe una plataforma de IoT de código abierto para el estudio del aseguramiento ante ataques DDoS, ni plataformas para realización de pruebas de estrés a bajo coste, ni conocimiento sobre botnets en dispositivos de IoT; se encuentra la necesidad de generar conocimiento libre y accesible sobre botnets heterogéneas y su aplicación en un entorno controlado, para de esta manera crear conciencia sobre la seguridad de los dispositivos de IoT y su aplicabilidad en sistemas distribuidos para realizar ataques DDoS sin el consentimiento del usuario. Gracias a su bajo coste, se ve la posibilidad de usar estos dispositivos para la ejecución de ataques coordinados en una botnet heterogénea.*

*En este artículo encontrará el desarrollo de un proyecto de software libre licenciado con GNU/GPLv3 para la interconexión de máquinas de distintas características (computadoras, dispositivos IoT, smartphones, tarjetas microcontroladas…) en una botnet de alta disponibilidad utilizando el protocolo MQTT, con nodos maestros intercambiables y asignación dinámica de cargas; destinada a realizar ataques de denegación de servicios del tipo get.*

*Se desea complementar el avance del proyecto, que se encuentra en fase de producción, para seguir añadiendo, en conjunto con el apoyo de la comunidad de software libre en seguridad informática.*

*Palabras Claves— Botmet, mqtt, IoT, tarjetas microcontroladas, Denegación distribuida de servicios, GNU/GPLv3, alta disponibilidad.*

# introducciÓn

En el campo de la seguridad informática, pareciera todo ser oscuro y con conocimientos inaccesibles para los menos enterados del tema.

Los interesados en aprender sobre seguridad informática no pueden acceder a toda la información, incluso en ocasiones se deben pagar costosos cursos para acceder a la misma; información que si bien estructurada técnicamente, en ocasiones llega a ser vacía en la práctica.

Además de la falta de libertad en la información, es importante destacar las falencias de seguridad en las infraestructuras nacientes, las cuales se van incorporando cada vez más rápidamente a la red; es importante destacar que estas vulnerabilidades pueden ser explotadas para diversos propósitos, sin embargo, los desarrolladores de estos productos no tienen mano firme para realizar mejoras en la seguridad de estos.

# Objetivos

1. *Objetivo general*

Generar una comunidad de software libre con base en un proyecto para la interconexión de máquinas en una Botnet destinada a realizar ataques de denegación distribuida de servicios (DDoS) de arquitectura redundante, con asignación dinámica de cargas y nodos maestros intercambiables.

1. *Objetivos específicos*

• Determinar las características de la conexión a utilizar entre distintas maquinas en una LAN.

• Diseñar algoritmos que sustenten el modelo de una Botnet con nodos maestros intercambiables y asignación dinámica de cargas.

• Integrar las partes lógicas y físicas del proyecto, aplicando el conjunto de normas de la licencia GNU/GPLv3 de software libre.

# Justificación

Teniendo en cuenta la creciente vinculación de dispositivos a internet, es importante pensar que estos deben ser robustos en cuanto a su infraestructura de seguridad. Para poder mejorarlas, se deben establecer soluciones mediante los análisis de vulnerabilidades, los cuales son precisamente irrupciones en la seguridad del sistema. Esto soportado por las comunidades de software libre, puede hacer que a la larga se generen mejores opciones para asegurar diferentes infraestructuras mediante la colaboración de las personas interesadas en este tipo de proyectos.

Cada vez se intenta solucionar más la necesidad de generar información libre y accesible a todo el mundo sobre el aseguramiento de brechas de seguridad. Las botnet heterogéneas y su aplicación real en un entorno controlado, pueden servir para concientizar a fabricantes y comunidades de software sobre las vulnerabilidades en dispositivos de IoT (Internet of Things), para así poder generar una comunidad de aprendizaje libre y descentralizado, y hacer de la red un lugar más seguro para navegar.

# Alcances

Se espera concluir el proyecto con una comunidad de software libre establecida, con la que en conjunto se haya desarrollado la implementación del sistema en tres tipos de máquinas distintas (computadores, tarjetas Nodemcu 8266 y dispositivos Android), con una infraestructura de clúster robusta y de alta disponibilidad. Se espera contar con una base de usuarios de la comunidad para desarrollar las diferentes adaptaciones del proyecto implementando IPv4 para los ataques a realizar.

# Resultados obtenidos hasta el momento

Botnet de alta disponibilidad, con arquitectura master-slave e identificación básica de cada nodo en la red.

Repositorio con proyecto 80% funcional en Python, y 50% funcional en Arduino [1].

# Webgrafía

[1] García, A. and Angarita, O. (2019). *BotnetsHeterogeneas*. [online] Github. Available at: https://intentodemusico.github.io/BotnetsHeterogeneas/ [Accessed 5 Jul. 2019].

# Referencias

Antonioli, D. (2018, febrero 1). [online] arxiv. Available at: https://arxiv.org/pdf/1802.00152.pdf

Bell, L. (2014, marzo 6). [online] The Inquirer. Available at: https://www.theinquirer.net/inquirer/news/2332589/bitcoin-mining-botnets-and-windows-xp-threats-are-booming-says-dell-sonicwall

Hispasec. (2018, octubre 1). [online] hispasec. Available at: https://unaaldia.hispasec.com/2018/10/torii-es-la-nueva-botnet-iot-multiplataforma.html

Kupreev, O., Strohschneider, J., & Khalimonenko, A. (2016). [online] securelist. Available at: https://securelist.com/analysis/quarterly-malware-reports/76464/ kaspersky-ddos-intelligence-report-for-q3-2016/

Osborne, C. (2018, septiembre 28). [online] zdnet. Available at: https://www.zdnet.com/article/meet-torii-a-new-iot-botnet-far-more-sophisticated-than-mirai/

panda security. (2018, marzo 9). [online] pandasecurity. Available at: https://www.pandasecurity.com/spain/mediacenter/malware/botnets/

Poor-man. (2016, octubre). [online] geektopia. Available at: https://www.geektopia.es/es/technology/2016/10/11/noticias/un-hacker-publica-el-codigo-de-un-programa-para-hacer-ataques-ddos.html

Rouse, M. (2014, enero). [online] techtarget. Available at: internetofthingsagenda: https://internetofthingsagenda.techtarget.com/definition/IoT-botnet-Internet-of-Things-botnet

Torres, J. (2014, octubre). [online] Hipertextual. Available at: https://hipertextual.com/archivo/2014/10/internet-cosas/

Vormayr, G., Zseby, T., & and Fabini, J. (2017). [online] Publikationsdatenbank der TU Wien. Available at: publik.tuwien.ac.at: https://publik.tuwien.ac.at/files/publik\_262720.pdf

1. Documento entregado el 5 de junio del 2019. Proyecto en desarrollo. [↑](#footnote-ref-1)