Detección de botnets utilizando herramientas Opensource

Lic Paula Venosa
pvenosa at info.unlp.edu.ar

Lic. Javier Díaz
jdiaz at info.unlp.edu.ar

LINTI (Laboratorio de Investigación en Nuevas Tecnologías Informáticas)
Facultad de Informática - UNLP
Calle 50 y 120 – 2do piso – La Plata, Buenos Aires, Argentina

Resumen

Las botnets representan una de las principales amenazas que afectan a las organizaciones y a los usuarios hoy en día. A través de las mismas los cibercriminales consiguen comprometer hosts sin el consentimiento de sus dueños, con el fin de usarlos como "trampolín" para el lanzamiento de distintos tipos de ataques hacia terceros, como ser denegación de servicio, fraude y robo de identidad entre otros.

En este artículo se presenta una línea de investigación que tiene como objetivo el estudio de las botnets y sus características, así como las técnicas de detección existentes, con sus ventajas y desventajas. El estudio incluye la búsqueda de herramientas que apliquen las técnicas investigadas con el fin de detectar botnets, y la creación de un ambiente de prueba en el cual se pueda testear y comparar el funcionamiento de dichas herramientas con el fin de proponer un framework o prototipo, implementado a partir de la combinación de las distintas herramientas que se consideren adecuadas para detección confiable y eficiente de botnets en una red.

Palabras clave: incidente de seguridad, bot, botnets, CERT[1] , opensource, detección

[1] Computer Emergency Response Team

Contexto

La línea de investigación presentada está inserta en el proyecto de incentivos "Redes, Seguridad y Desarrollo de Aplicaciones para e-educación, e-salud, e-gobierno y e-inclusión" del LINTI[2] de la Facultad de Informática de la Universidad Nacional de La Plata (UNLP). En el marco de este proyecto un grupo de docentes/investigadores del LINTI trabajan en temas relacionados a la prevención, detección y mitigación de incidentes de seguridad.

El estudio de las botnets y sus características, así como la investigación respecto a las técnicas de detección y mitigación, y el desarrollo y uso de herramientas relacionadas, constituye un tema de vital importancia en el área. [1]

Esta línea también representa un tema de interés en el marco del acuerdo de cooperación establecido en el año 2012 a través del proyecto "Infraestructuras Seguras para Gobierno Electrónico" entre el GASS[3] y el LINTI de la Facultad de Informática de la UNLP.

[2] LINTI (Laboratorio de Investigación en Nuevas Tecnologías Informáticas) – www.linti.unlp.edu.ar

[3] Grupo de Análisis, Seguridad y Sistemas – Universidad Complutense de Madrid – gass.ucm.es

Introducción

Hoy en día los ataques en Internet han sufrido una transformación profunda, mientras que hace un tiempo se concentraban en afectar la disponibilidad de la Infraestructura y los servicios, hoy tienen como objetivo también a las personas y a las organizaciones. Detrás de estos nuevos ataques existen hosts comprometidos, ubicados en hogares, escuelas, organizaciones privadas y gubernamentales;que están infectados con un bot[4] que se comunica con un bot controller y otros bots que forman lo que comunmente se conoce como botnet o zombie army[2]. Es la presencia de un canal de comunicación con un controlador, lo que diferencia a los botnets de otros tipos de ataques.

Las botnets son usadas para llevar a cabo distintos tipos de actividades maliciosas: ataques de denegación de servicio, fraude, robo de identidad, recolección de información confidencial, etc [3].

Las botnets representan, actualmente, un problema real [4] y de rápida evolución. Constituyen una de las amenazas de seguridad más preocupantes debido a que causan enormes pérdidas financieras y graves daños a las organizaciones de todo el mundo y se encuentran en constante evolución [3][5].

Muchos son los ejemplos de botnets que podemos citar desde su aparición asociada por algunos autores al cambio de milenio[6]. Entre los más recientes podemos mencionar botnets usadas para distribuir malware, como VIRUT [7], así como otras que controlan millones de teléfonos Android [8] posibilitando entre otras cosas la extracción de información confidencial del usuario o la descarga automática de aplicaciones sin el consentimiento del mismo.

Si bien existen varias iniciativas e investigaciones sobre este tema, aún existen interrogantes, pruebas a realizar y soluciones para proponer en cuanto a técnicas de prevención, detección y combinación de herramientas posibles para ello [9].

Como primer paso al abordar este tema es fundamental entender las características de las botnets: sus componentes, las arquitecturas existentes y su funcionamiento.

El análisis de comportamiento puede realizarse utilizando capturas de tráfico de una red en funcionamiento o simulando ambientes donde las distintas botnets se ejecutan [10].

En lo que se refiere a detección, existen numerosas técnicas y distintas clasificaciones para las mismas. Algunos autores hablan de técnicas pasivas y técnicas activas [11]. Las técnicas pasivas consisten en obtener datos a partir del monitoreo [12], sin interferir en el ambiente ni alterar la evidencia, mientras que las activas incluyen la interacción con los recursos que están siendo monitoreados.

Más allá de las técnicas que se utilicen, numerosos son los desafíos a los que nos enfrentaremos al evaluar las mismas así como las herramientas existentes para detectar botnets, al igual que ocurre con la investigación relacionada a detección de intrusiones en general [13], entre ellas:

- la dificultad de modelar con un conjunto de trazas la realidad de Internet, debido a que las redes son controladas por diferentes organizaciones que son de distinta naturaleza (académicas, corporativas) y que tienen

[4] El término bot deriva de ro-bot". Bot es un termino genérico usado para describir un script diseñaado para ejecutar funciones predefinidas de forma automatizada

distintos objetivos, intereses y políticas; eso sumado a que la tendencia es la reserva a la hora de compartir información.

- El conflicto que existe entre el estudio de las amenazas y las redes implicadas, y el mantenimiento de la privacidad de la información sensible que las redes trasmiten que incluye acciones y comunicaciones de los usuarios de las mismas .

Con esta problemática y desafíos nos encontramos al plantear este proyecto, teniendo como ámbito de trabajo la red de la UNLP, y abordando esta línea de investigación desde la visión de un centro de respuesta de incidentes, sin perder de vista los objetivos que el mismo tiene respecto a la prevención, detección y mitigación de incidentes de seguridad.

Líneas de Investigación, Desarrollo e Innovación

Actualmente las tareas a realizar en en el marco de la presente investigación tienen que ver con la búsqueda de herramientas opensource que apliquen las técnicas estudiadas con el fin de detectar botnets, y la creación de un ambiente de prueba que simule la problemática y permita comparar el funcionamiento de dichas herramientas.

También nos encontramos en el proceso de definir los escenarios en los cuales se estudiará el problema en forma concreta, creando así el ambiente de trabajo de la siguiente etapa.

Es importante considerar también los aportes de las soluciones posibles en relación la implementación de controles de seguridad en el marco de las normas ISO 27000 [14].

Resultados y Objetivos

En cuanto a los resultados hasta el momento alcanzados:

- Se estudiaron características y arquitecturas de las botnets.
- Se investigaron las técnicas de detección de botents existentes.
- Se recabó información respecto a herramientas existentes, entre las que se encuentran:
    - ***botnets*** [15]: una herramienta opensource, con licencia gnugpl. La misma se compone de un conjunto se scripts escritos en python que reciben streams de datos (netflow) y generan alertas cuando detectan actividad sospechosa
    - ***botminer*** [16]: un prototipo desarrollado por investigadores del College of Computing, Georgia Institute of Technology. Este framework basa su funcionamiento partiendo de la premisa de que en una botnet, los bots se comunican con su servidor y sus pares, y ejecutan actividades maliciosas y , siguiendo patrones de comunicación y de actividad maliciosa.

- ***Nsgbot*** [17]***:*** una herramienta opensource, con licencia gnugpl. La misma cuenta con 3 módulos: ngsbotHTTP, ngsbotIRC y ngsbotDNS; los cuales permiten detectar botnets analizando el tráfico HTTP, IRC y DNS respectivamente.

- ***Ourmon*** [18]***:*** una herramienta opensource que analiza el tráfico de red y detecta anomalías, orientada a la estadística. Las botnets se encuentran incluídas dentro de las anomalías que detecta.

- ***Bothunter*** [19] es una herramienta que a pesar de no ser opensource se encuentra disponible en forma libre y gratuita.

  La misma es una modificación sobre snort, a partir del agregado de módulos que permiten la detección de botnets.

El objetivo al que apunta la presente línea de investigación es la propuesta de un framework o prototipo, implementado a partir de la combinación de las distintas herramientas que se consideren adecuadas para detección confiable y eficiente de botnets en una red.

Formación de Recursos Humanos

La línea de investigación descripta se encuentra en el marco de la realización de la tesis de master de Redes de Datos de la Profesora Paula Venosa, la cual forma parte de las actividades llevadas a cabo por CERT-UNLP[5], que junto con cert.br[6] de Brasil y UNAM-CERT[7] tienen como objetivo analizar las estrategias de tratamiento de botnets para combatir malware y spam.

Los resultados del presente estudio servirán para fortalecer el conocimiento del grupo del CERT Académico de la Universidad Nacional de La Plata, compuesto por 3 alumnos avanzados de la Facultad de Informática de la UNLP y coordinado por un grupo de docentes e investigadores especialistas en Seguridad en Redes del LINTI, bajo la dirección del Lic. Javier Díaz. Este grupo trabaja desde el año 2008 en la prevención, detección y mitigación de incidentes de seguridad [20]. Con los resultados obtenidos se espera enriquecer las tareas del Cert.unlp, aportando metodología y utilización de nuevas herramientas.

Asimismo lo aprendido durante el transcurso del presente proyecto podrá ser aprovechado por los docentes del grupo en la elaboración de propuestas de tesinas a desarrollar en la Facultad de Informática de la UNLP.

[5] http://www.cespi.unlp.edu.ar/cert

[6] http://www.cert.br/

[7] www.cert.org.mx/

Referencias

[1] “Botnet the Silent Threat” , David Barroso (S21sec, Spain), ENISA

[2] “The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets” - Evan Cooke,Farnam Jahanian, Danny McPherson. , Electrical Engineering Computer Science Department - Arbor Networks -University of Michigan

[3] “Botnet Literature Review”, Brandon Shirley, Utah State Univeristy, Logan, Utah

[4] “Daily botnets statistics” - http://botnet-tracker.blogspot.com.ar/

[5] “Botnets and cybercrime Introduction”- http://resources.infosecinstitute.com/botnets-and-cybercrime-introduction/

[6] “The evolution of the botnet” http://www.itpro.co.uk/627487/the-evolution-of-the-botnet

[7] “Cae la botnet Virut, responsable de infectar 300.000 ordenadores” http://www.siliconweek.es/noticias/cae-la-botnet-virut-responsable-de-infectar-300-000-ordenadores-32288

[8] “Botnet amenaza a 150 millones de usuarios de Android” - http://www.csirtcv.gva.es/es/noticias/botnet-amenaza-150-millones-de-usuarios-de-android.html

[9] “Botnets: 10 Tough Questions” , Daniel Plohmann - Elmar Gerhards-Padilla - Felix Leder, ENISA

[10] “Botnet Lab Creation with Open Source Tools and usefulness of such a tool for researchers”, Dimitris Vergos, Rochester Institute of Technology B. Thomas Golisano College Of Computing and Information Sciences

[11]“Botnets: Detection, Measurement, Disinfection & Defence”, Daniel Plohmann - Elmar Gerhards-Padilla - Felix Leder, ENISA

[12] “ A Distributed Botnet Detecting Approach Based on Traffic Flow Analysis”, Li Sheng, Liu Zhiming, He Jin, Deng Gaoming, Huan Wen, Northern Electronic Instrument Institute,

[13] “Challenges in Experimenting with Botnet Detection Systems” Adam J. Aviv Andreas Haeberlen, University of Pennsylvania

[14] ISO/IEC 27001:2005 - Sistemas de gestion de seguridad de la información-Requerimientos-Anexo A Controles

[15] https://code.google.com/botnets

[16] “BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection” Guofei Gu, Roberto Perdisci, Junjie Zhang, and Wenke Lee, College of Computing, Georgia Institute of Technology, USA

[17]http://www.findbestopensource.com/product/nsgbot

[18] http://ourmon.sourceforge.net/

[19] http://www.bothunter.net

[20] “Tendencias en incidentes de seguridad atendidos por el CERT académico Cert-UNLP” -Einar Lanfranco, Nicolás Macia, Paula Venosa, Lía Molinari, Javier Díaz-WICC 2010