

Botnet a través de Twitter

A lo largo del tiempo se han conocido muchos casos e incidentes de seguridad donde los actores principales son las botnets, y cuyo proceso de reclutamiento de equipos infectados centra sus esfuerzos en explotar las tecnologías con mayor popularidad, entre las que hemos destacado las redes sociales.

Incluso casos donde la comunicación entre el botmaster y los zombis (C&C) se realiza a través de la red de microblogging más conocida: Twitter. A lo que cabe la pregunta ¿cómo logran los delincuentes automatizar este proceso?

En las últimas horas hemos detectado una aplicación que se encuentra *in-the-wild*, desarrollada para automatizar la creación de botnets a través de la popular red social. ../..

Esta es una aplicación muy sencilla diseñada para automatizar la creación de troyanos del tipo bot: el desarrollo de estos programas buscan ser lo más intuitivo posible y crear aplicaciones para principiantes (*point-and-click*), como esta, que solo requiere registrar un perfil en Twitter que será utilizado en forma dañina para lanzar los comandos al equipo infectado.

Para construir el malware, el atacante sólo debe indicar el nombre de usuario que mandará las instrucciones a los equipos zombis. El malware que se genera a través de dicho constructor es el código malicioso que, al infectar un sistema, recibirá los comandos lanzados a través del perfil en la red social. Es decir, el atacante podrá controlar los equipos infectados a través de los contenidos que escriba en su perfil de Twitter.

El bot creado posee una serie de comandos básicos que permiten al *botmaster* interactuar con las computadoras comprometidas. Por ejemplo, entre muchos otros:

- el comando **.DDOS*IP*PUERTO** realiza un Ataque de Denegación de Servicio Distribuida (DDoS)
- con **.DOWNLOAD*ENLACE/MALWARE.EXE** se descarga otro código malicioso
- **.VISIT*ENLACE** abre el enlace en el navegador del usuario
- el comando **.REMOVEALL** elimina automáticamente la información de la botnet y el perfil de Twitter

Al analizar el código y ver su comportamiento, queda en evidencia que el creador del malware ha cometido algunos errores como publicar su cuenta de Twitter o generar un archivo corrupto dadas ciertas circunstancias. Esto demuestra que esta es una versión que será mejorada en el futuro cercano, abriendo la posibilidad de nuevos tipos de amenazas.

Para graficar mejor el proceso, hemos desarrollado un video educativo donde podrán observar todo el proceso, desde la creación del malware por parte del atacante, la infección en el sistema de la víctima y el envío de instrucciones para la realización de un Ataque de Denegación de Servicio Distribuido. En el video podrán observar todas las explicaciones paso a paso del proceso de ataque.

Es interesante mencionar que este bot abre una nueva puerta no considerada hasta el momento, **la posibilidad de controlar una botnet a través de cualquier tipo de dispositivo que tenga acceso a Twitter** o a sus APIs (actualmente cualquier tipo de teléfono por ejemplo) ya que el comando en el sistema infectado será ejecutado sin importar de donde provenga el mismo.

Vale mencionar que los usuarios de cualquiera de los productos de ESET pueden estar tranquilos con la seguridad de sus sistemas ya que esta amenaza es detectada de forma proactiva a través de su motor ThreatSense.

Fecha: 14/05/2010

Fuente: blogs.eset-la.com