Android botnets for multi targeted attacks

Jaime García González y Adán Cano Moreno

2 de abril de 2019

Universidad Carlos III de Madrid

Contenido

Información del artículo

Valentin Hamon

- Ingeniero de Seguridad informática de Sistemas por la ESIEA.
- En ese momento: Estudiante e investigador en ESIEA.
- Actualidad: FAMOCO
- Otros artículos: *Malicious URI Resolving in PDFs* (muestra como una petición HTTP desde un PDF puede ser una buena herramienta para un atacante)

Springer-Verlag

- Filial francesa de Springer, fundada en 1986.
- Ámbito: medicina, matemáticas, estadística, informática e ingeniería.
- Otras actividades: publicación de libros del campo de las ciencias y editorial Springer en Francia.

Contenido del artículo

Introducción

- Los dispositivos móviles tienen muchos sensores que son atractivos para los atacantes –> acceso a través de las aplicaciones.
- Prescripción del procedimiento a seguir para realizar un ataque botnet sobre distintos dispositivos móviles Android al mismo tiempo para capturar información.
- Objetivo: exponer el potencial que tiene este tipo de ataques y el peligro que puede suponer.
- Ejemplo de ataque: mostrar la localización de diferentes dispositivos móviles a través de diferentes fases.

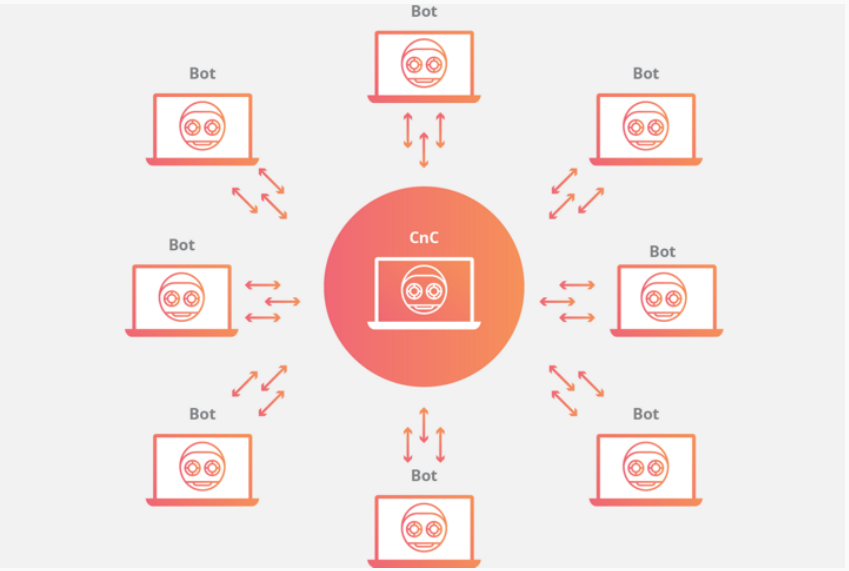
Fases

El artículo divide el procedimiento de ataque en 5 fases:

- Recoger información
- Almacenamiento y gestión de la información
- Mostrar la información
- Información de verificación
- Determinar puntos de encuentro entre dispositivos

Fases: Recoger información

- Ataque botnet: cualquier grupo de dispositivos infectados y controlados por un atacante de forma remota.
- Usos: ataques de denegación de servicio distribuidos (DDoS), envío de Spam, minería de Bitcoins y robo de Bitcoins.
- Ejemplos: Conficker, Zeus, Waledac, Mariposa y Kelihos.



Fases: Recoger información

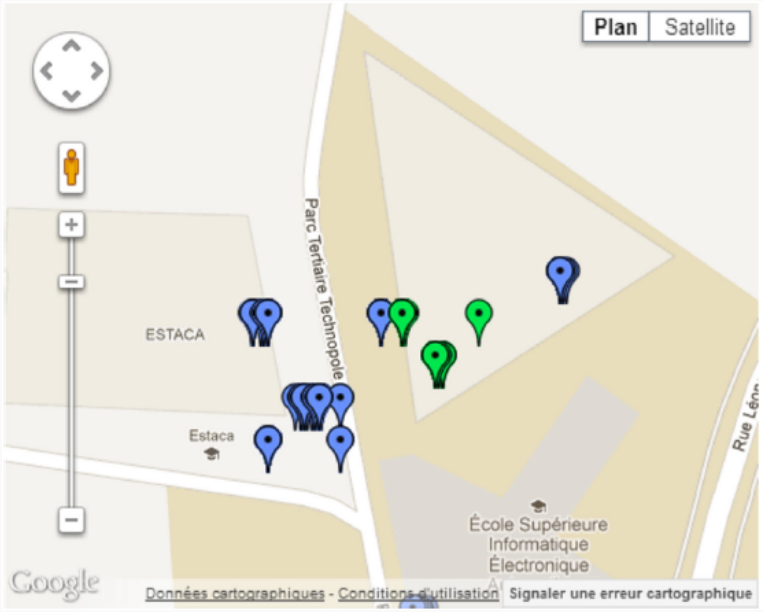
- Se necesita que el teléfono esté encendido el mayor tiempo posible.
- Se necesita una red de bots móvil para enviar datos de geolocalización al servidor –> se crea una instancia de nuestra clase de LocationListener al comenzar la actividad principal.
- Se genera un protocolo para enviar los datos recogidos en una sola cadena.
- Es posible transferir datos de dos maneras diferentes recogidos de los smartphones a un servidor –> HTTP o SMS.

Fases: Almacenamiento y gestión de la información

- PHP o MySQL para gestionar la información –> instalados por defectos en la red de servidores mundial.
- Se concatenan todas las variables a almacenar en una única cadena (localización, fecha...).
- Primera idea para almacenar los datos: crear para cada botnet una nueva tabla con el IMEI (*International Mobile Equipment Identity*) como nombre –> problema cuando intentamos crear una nueva tabla con un número como nombre (no permitido en MySQL).
- Solución: traducimos los números de IMEI en caracteres (0 = a, 1 = b, ...). IMEI es único –> n tablas con n nombres diferentes.

Fases: Mostrar la información

- Incluir el encabezado de una web HTML con algunas líneas para inicializar la API de Google maps.
- Se inicializa una matriz para tener diferentes colores para nuestros marcadores en el mapa.
- Consulta SELECT a los IMEIs. Usamos *fecth()* de PHP para acceder a cada línea de la tabla y almacenamos los nombres de tablas en un array para poder hacer consultas en todas las tablas de botnets.

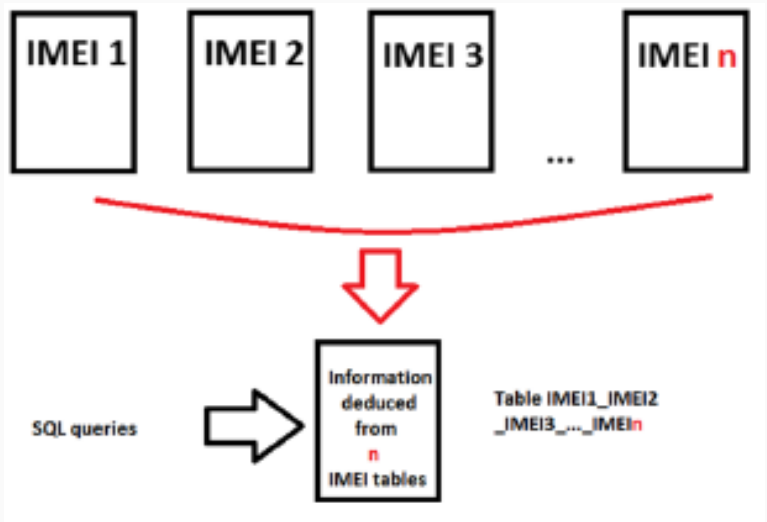


Fases: Información de verificación

- Determinar el comportamiento de las personas infectadas –> si las víctimas están en un autobús, en un tren, andando o paradas. Tenemos que determinar la velocidad de movimiento de nuestras víctimas.
- Problema: recopilar suficientes datos para determinar el comportamiento de la víctima.
- Antes de analizar cualquier comportamiento se debe comprobar los datos. Se crea una nueva tabla con un nombre que es la concatenación de los nombres de las n tablas separados por "_".
- La fecha será un atributo único en la tabla (sólo tenemos una geolocalización entrada de datos en la base de datos por segundo).

Fases: Información de verificación

- Podemos separar los datos de todas nuestras redes de bots por cualquier período de tiempo.
- Podemos mostrar en el mapa datos de nuestras redes de bots con respecto a una fecha precisa.
- Podemos seleccionar y mostrar datos de múltiples objetivos con criterios muy específicos (a través de la fecha.



Fases: Determinar puntos de encuentro entre dispositivos

Android botnets for multi targeted attacks

Jaime García González y Adán Cano Moreno

2 de abril de 2019

Universidad Carlos III de Madrid