DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico

Malware de Android

22 de julio de 2015

Seguridad Informática
1er Cuatrimestre de 2015

Integrante	LU	Correo electrónico
Castro, Alan		alancastro90@gmail.com
Kujawski, Kevin	459/10	kevinkuja@gmail.com
Ortíz de Zárate, Juan Manuel		jmanuoz@gmail.com
Vanecek, Juan	169/10	juann.vanecek@gmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
http://www.fcen.uba.ar

Índice

1. Introducción

Se nos presentó el desafío de crear un Malware para Android que simulando ser una aplicación normal por atrás le robe información al usuario del dispositivo. Entre una serie de varias opciones para robar decidimos 2, robar los contactos y la ubicación del dispositivo, para luego armar el historial de ubicaciones.

2. Herramientas utilizadas

Para trabajar con Android vamos a necesitar el SDK, un emulador para celulares, y un entorno de programación. Todo esto viene incluido en un paquete fácil de utilizar. Comenzamos entonces descargando el ADT Bundle (http://developer.android.com/sdk/index.html) que incluye los componentes esenciales del SKD de Android y una versión del Eclipse que incorpora ADT (Android Development Tools) para agilizar el desarrollo de aplicaciones Android. La herramienta incluye el emulador que utilizamos para simular que estamos trabajando sobre un celular y poder hacer las verificaciones más rápidamente. Para correrlo hay que seleccionar un dispositivo, nosotros utilizamos el Nexus One que es un celular básico.

Por otro lado para el servicio no hace falta utilizar algo tan pesado como otro Eclipse, así que preferimos utilizar una aplicación en PHP. Para ello necesitamos un servidor. El WAMP (Windows Apache MySql PHP) monta un servidor completo en Windows de manera muy sencilla, simplemente instalándolo y corriéndolo Ahora sí, podemos levantar el servidor y tener la aplicación funcionando. Para esto solo necesitamos copiar la carpeta del servidor en la carpeta www que se encuentra en el directorio en donde se instaló el WAMP

3. Aplicación

3.1. Cliente

3.2. Servidor

El servidor es el que se encarga de recibir los datos que le envia la aplicacion, guardarlos y posteriormente mostrarlo. El mismo esta desarrollado en PHP, utilizando Bootstrap como framework de diseño y GoogleMaps para la funcionalidad del mapa, la información es guardada en archivos de texto. El servidor tiene dos archivos diferentes para recibir los distintos tipos de información, él mismo lee por POST los parámetros que el servidor le envia en tipo JSON, lo decodifica y lo guarda. Además cuenta con una pantalla para mostrar toda la información que fue recogiendo:

4. Dificultades

A lo largo del desarrollo del malware no tuvimos muchas dificultades, solamente fue una lucha constante con las limitaciones que atrae utilizar un emulador para utilizar el malware, como puede ser que no reconozca un GPS y haya que enviarle la información por otro lado, configurar el servicio para que cada tanta cantidad de tiempo realice el envío (internamente por localhost) y el testeo de que se inicie apenas se prenda el telefono. A pesar de eso, en cuestiones de visualización, logica y acceso a la información a robar no tuvimos problema.

5. Mejoras

- Configuración de la IP del server.
- Configurar el tiempo de envio de la información. Actualmente esta fijo en 10 segundos, factor que podria generar que se note la sobrecarga y por consiguiente que se detecte el malware
- Mejorar el servidor visualmente
- Lograr identificar el dispositivo. Ya sea por un login o por la MAC del dispositivo