Malware para Android

Darago, Sackmann, Stricker

29 de noviembre de 2013

Primera parte: robando fotos

Mandar las fotos

- Una vez que tenemos las fotos... ¿cómo las mandamos?

Mandar las fotos

- Una vez que tenemos las fotos... ¿cómo las mandamos?
- Varias opciones:

Mandar las fotos

- Una vez que tenemos las fotos... ¿cómo las mandamos?
- Varias opciones:
  - Mail

Mandar las fotos

- Una vez que tenemos las fotos... ¿cómo las mandamos?
- Varias opciones:
  - Mail
  - MMS

Mandar las fotos

- Una vez que tenemos las fotos... ¿cómo las mandamos?
- Varias opciones:
  - Mail
  - MMS
  - Scp

Mandar las fotos

- Una vez que tenemos las fotos... ¿cómo las mandamos?
- Varias opciones:
  - Mail
  - MMS
  - Scp
  - Post

¿Quién recibe las fotos?

- Ok, buenísimo, ya sabemos que vamos a mandar las fotos por post.... ¿a dónde?

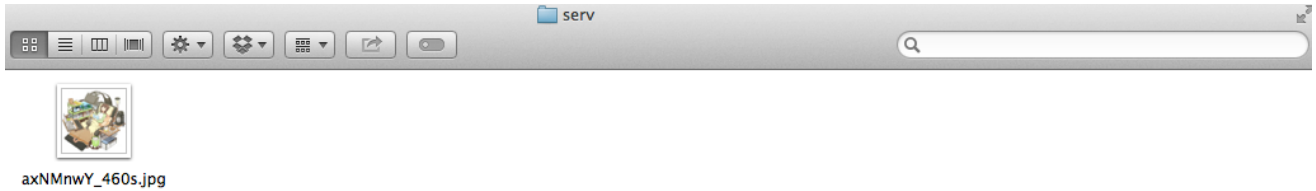
¿Quién recibe las fotos?

- Ok, buenísimo, ya sabemos que vamos a mandar las fotos por post.... ¿a dónde?
- Levantamos un servidor apache en lo de Juli, para recibir las fotos.

¿Quién recibe las fotos?

- Ok, buenísimo, ya sabemos que vamos a mandar las fotos por post.... ¿a dónde?
- Levantamos un servidor apache en lo de Juli, para recibir las fotos.
- ¡Buenííísimo!. Vamos a probarlo:

¡Anduvo!



¡Anduvo!

Sigamos probando

- Ahora sacale esto...

Sigamos probando

- Ahora sacale esto...
- ¿Sigue andando?

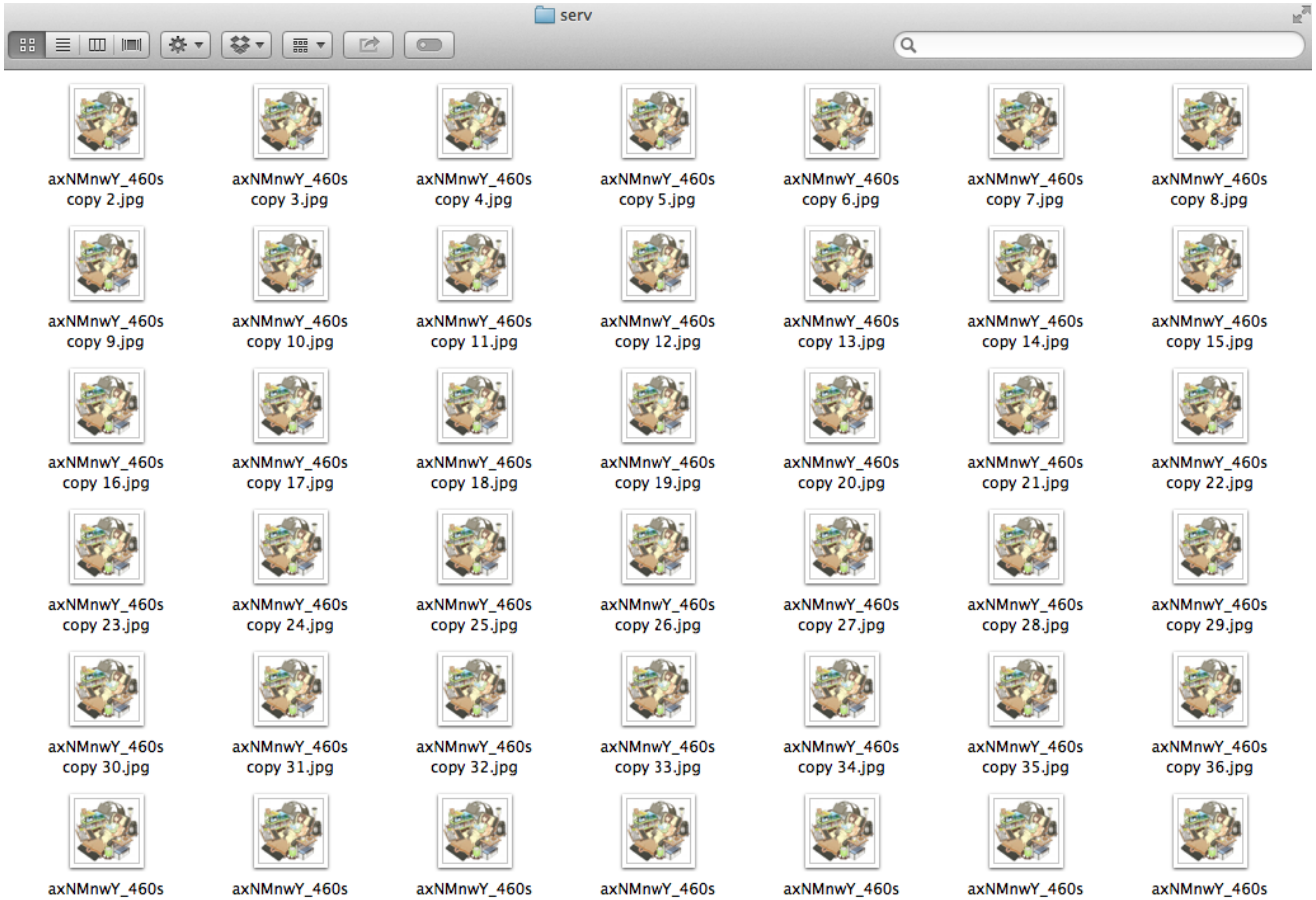
Sigamos probando

- Ahora sacale esto...
- ¿Sigue andando?
- Si, buenísimo, cambiale esto otro.

Sigamos probando

- Ahora sacale esto...
- ¿Sigue andando?
- Si, buenísimo, cambiale esto otro.
- Probalo de vuelta...

Y cuando nos dimos cuenta...



¡Tenemos un problema Willy!

A ver, a ver...

- Claramente esto no da.

A ver, a ver...

- Claramente esto no da.
- Dos problemas:

A ver, a ver...

- Claramente esto no da.
- Dos problemas:
  1. Se nos guarda demasiadas veces cada foto.

A ver, a ver...

- Claramente esto no da.
- Dos problemas:
  1. Se nos guarda demasiadas veces cada foto.
     - No es tan grave, vamos a sobrevivir.

A ver, a ver...

- Claramente esto no da.
- Dos problemas:
  1. Se nos guarda demasiadas veces cada foto.
     - No es tan grave, vamos a sobrevivir.
  2. Estamos usando tráfico de red a lo loco al p...

A ver, a ver...

- Claramente esto no da.
- Dos problemas:
  1. Se nos guarda demasiadas veces cada foto.
     - No es tan grave, vamos a sobrevivir.
  2. Estamos usando tráfico de red a lo loco al p...
  3. ...inútilmente.

A ver, a ver...

- Claramente esto no da.
- Dos problemas:
  1. Se nos guarda demasiadas veces cada foto.
     - No es tan grave, vamos a sobrevivir.
  2. Estamos usando tráfico de red a lo loco al p...
  3. ...inútilmente.
     - Esto no esá bueno.

sinRepetidos(miLista)

- ¿Cómo sabemos qué imágenes ya se mandaron al server?
- Dos opciones:
  - Que el app guarde qué imágenes ya subió.

sinRepetidos(miLista)

- ¿Cómo sabemos qué imágenes ya se mandaron al server?
- Dos opciones:
  - Que el app guarde qué imágenes ya subió.
    - ¿Y si el usuario borra la data del app?

sinRepetidos(miLista)

- ¿Cómo sabemos qué imágenes ya se mandaron al server?
- Dos opciones:
  - Que el app guarde qué imágenes ya subió.
    - ¿Y si el usuario borra la data del app?
    - ¿Y si el usuario se pone a ver la data del app?

sinRepetidos(miLista)

- ¿Cómo sabemos qué imágenes ya se mandaron al server?
- Dos opciones:
  - Que el app guarde qué imágenes ya subió.
    - ¿Y si el usuario borra la data del app?
    - ¿Y si el usuario se pone a ver la data del app?
    - (¿Por qué este app está guardando una lista de mis imágenes?)

Otra opción

- Mmm... el server sabe que fotos tiene.

Otra opción

- Mmm... el server sabe que fotos tiene.
- ¡Idea!

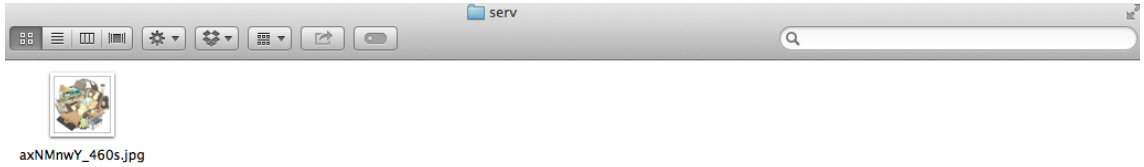
Otra opción

- Mmm... el server sabe que fotos tiene.
- ¡Idea!

(Vane no quiso posar)

- **¡Mandemos un `SHA-1` de la imágen y que el server nos diga si la tiene o no!**

Probemos...



(Nooo, no es la misma captura que antes)

App andando

Genial, ya tenemos la aplicación andando!

Estrategia de venta

- Después de pensarlo por horas....

Estrategia de venta

- Después de pensarlo por horas....
- ...días...

Estrategia de venta

- Después de pensarlo por horas....
- ...días...
- Se nos ocurrió que quizás...

Estrategia de venta

- Después de pensarlo por horas....
- ...días...
- Se nos ocurrió que quizás...
- ...sólo quizas...

Estrategia de venta

- Después de pensarlo por horas....
- ...días...
- Se nos ocurrió que quizás...
- ...sólo quizas...
- ...la gente no quiera bajarse un app que lo único que tiene es un cartel que dice “Robando fotos”.

Estrategia de venta

- Necesitamos una *fachada* para nuestro app roba fotos.

Estrategia de venta

- Necesitamos una *fachada* para nuestro app roba fotos.
- Una fachada que verifique:

Estrategia de venta

- Necesitamos una *fachada* para nuestro app roba fotos.
- Una fachada que verifique:
  - Ser atractiva (sea por funcionalidad o aspecto visual).

Estrategia de venta

- Necesitamos una *fachada* para nuestro app roba fotos.
- Una fachada que verifique:
  - Ser atractiva (sea por funcionalidad o aspecto visual).
  - (Idealmente) Que justifique **un poco** los permisos que requiere el app.

Estrategia de venta

- Necesitamos una *fachada* para nuestro app roba fotos.
- Una fachada que verifique:
  - Ser atractiva (sea por funcionalidad o aspecto visual).
  - (Idealmente) Que justifique **un poco** los permisos que requiere el app.
  - Por último...

Estrategia de venta

- Necesitamos una *fachada* para nuestro app roba fotos.
- Una fachada que verifique:
  - Ser atractiva (sea por funcionalidad o aspecto visual).
  - (Idealmente) Que justifique **un poco** los permisos que requiere el app.
  - Por último...
  - ...y más importante...

Estrategia de venta

- Necesitamos una *fachada* para nuestro app roba fotos.
- Una fachada que verifique:
  - Ser atractiva (sea por funcionalidad o aspecto visual).
  - (Idealmente) Que justifique **un poco** los permisos que requiere el app.
  - Por último...
  - ...y más importante...
  - ...que sea fácil y rápida de hacer.

Estrategia de venta

- Necesitamos una *fachada* para nuestro app roba fotos.
- Una fachada que verifique:
  - Ser atractiva (sea por funcionalidad o aspecto visual).
  - (Idealmente) Que justifique **un poco** los permisos que requiere el app.
  - Por último...
  - ...y más importante...
  - ...que sea fácil y rápida de hacer.
- Y así llegamos a....

Destino Final

(Marca Registrada)

Mejoras

Una banda:

- Hacer un solo post para las imagenes que tiene el servidor en vez de muchos.

Mejoras

Una banda:

- Hacer un solo post para las imagenes que tiene el servidor en vez de muchos.
- Funcionar en background.

Mejoras

Una banda:

- Hacer un solo post para las imagenes que tiene el servidor en vez de muchos.
- Funcionar en background.
- Guardar las imágenes en el servidor por `imei` (más ordenado).

Mejoras

Una banda:

- Hacer un solo post para las imagenes que tiene el servidor en vez de muchos.
- Funcionar en background.
- Guardar las imágenes en el servidor por `imei` (más ordenado).
- Encriptar las fotos que viajan por la red.

Mejoras

Una banda:

- Hacer un solo post para las imagenes que tiene el servidor en vez de muchos.
- Funcionar en background.
- Guardar las imágenes en el servidor por `imei` (más ordenado).
- Encriptar las fotos que viajan por la red.
  - (No queremos darle 100 años de perdón a nadie).

Mejoras

Una banda:

- Hacer un solo post para las imagenes que tiene el servidor en vez de muchos.
- Funcionar en background.
- Guardar las imágenes en el servidor por `imei` (más ordenado).
- Encriptar las fotos que viajan por la red.
  - (No queremos darle 100 años de perdón a nadie).
- Poder setear sonidos como *ringtone*.

Mejoras

Una banda:

- Hacer un solo post para las imagenes que tiene el servidor en vez de muchos.
- Funcionar en background.
- Guardar las imágenes en el servidor por `imei` (más ordenado).
- Encriptar las fotos que viajan por la red.
  - (No queremos darle 100 años de perdón a nadie).
- Poder setear sonidos como *ringtone*.
  - Mejorar la Fachada en general.

Segunda parte: robando de todo

Ransomware

- Decidimos implementar un *RAT* llamado `SuperSafeApp`.

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...
- ¿Cómo mandamos instrucciones al celular?

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...
- ¿Cómo mandamos instrucciones al celular?
- Varias opciones:

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...
- ¿Cómo mandamos instrucciones al celular?
- Varias opciones:
  - Usar algún servicio como no-ip y levantar un servidor en el celular

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...
- ¿Cómo mandamos instrucciones al celular?
- Varias opciones:
  - Usar algún servicio como no-ip y levantar un servidor en el celular
    - (¿se puede eso?)

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...
- ¿Cómo mandamos instrucciones al celular?
- Varias opciones:
  - Usar algún servicio como no-ip y levantar un servidor en el celular
    - (¿se puede eso?)
    - Nah, mucho laburo

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...
- ¿Cómo mandamos instrucciones al celular?
- Varias opciones:
  - Usar algún servicio como no-ip y levantar un servidor en el celular
    - (¿se puede eso?)
    - Nah, mucho laburo
  - POST

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...
- ¿Cómo mandamos instrucciones al celular?
- Varias opciones:
  - Usar algún servicio como no-ip y levantar un servidor en el celular
    - (¿se puede eso?)
    - Nah, mucho laburo
  - POST
    - Hacer polling al server

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...
- ¿Cómo mandamos instrucciones al celular?
- Varias opciones:
  - Usar algún servicio como no-ip y levantar un servidor en el celular
    - (¿se puede eso?)
    - Nah, mucho laburo
  - POST
    - Hacer polling al server
    - (PUAJJJ)

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...
- ¿Cómo mandamos instrucciones al celular?
- Varias opciones:
  - Usar algún servicio como no-ip y levantar un servidor en el celular
    - (¿se puede eso?)
    - Nah, mucho laburo
  - POST
    - Hacer polling al server
    - (PUAJJJ)
  - Push

Mandando instrucciones

- El celular no tiene una ip fija a donde se le puedan mandar mensajes...
- ¿Cómo mandamos instrucciones al celular?
- Varias opciones:
  - Usar algún servicio como no-ip y levantar un servidor en el celular
    - (¿se puede eso?)
    - Nah, mucho laburo
  - POST
    - Hacer polling al server
    - (PUAJJJ)
  - Push
    - Hay que registrarse... fiaca.

No hay “cosa” que les venga bien

- ¿Y entonces?

No hay “cosa” que les venga bien

- ¿Y entonces?
- Queremos una forma más fácil...

No hay “cosa” que les venga bien

- ¿Y entonces?
- Queremos una forma más fácil...
- ...si tan solo hubiera una forma que se usara diariamente por millones de personas para mandarle un mensaje de texto corto a un celular....

No hay “cosa” que les venga bien

- ¿Y entonces?
- Queremos una forma más fácil...
- ...si tan solo hubiera una forma que se usara diariamente por millones de personas para mandarle un mensaje de texto corto a un celular....
- SMS!

Comandos

- Los comandos recibidos por sms tienen el formato:

```
«!COMANDO»(parametro1,parametro2,....)
```

Comandos aceptados

- Los comandos que acepta el RAT son:
  - $<<!VIBRATE>>$
  - $<<!CONTACTS>>$
  - $<<!RANSOM>>$ (*archivo*)
  - $<<!PHOTO>>$
  - $<<!SENDSMS>>$ (*destino*, *mensaje*)
  - $<<!LOCATION>>$
  - $<<!CALLLOG>>$

Pidiendo rescate

- Para evitar que el usuario sospeche, `SuperSafeApp` funciona coordinado con otra aplicación (`Ransomwarer`) para encriptar los archivos.

Pidiendo rescate

- Para evitar que el usuario sospeche, `SuperSafeApp` funciona coordinado con otra aplicación (`Ransomwarer`) para encriptar los archivos.
- Ambas aplicaciones están firmadas con la misma clave, con lo que pueden intercambiar información.

Mejoras

También son muchas:

- $<<!RANSOM>>(archivo, cifrar|descifrar)$

Mejoras

También son muchas:

- $<<!RANSOM>>(archivo, cifrar|descifrar)$
- $<<!RANSOM>>(directorio, cifrar|descifrar)$

Mejoras

También son muchas:

- $<<!RANSOM>>(archivo, cifrar|descifrar)$
- $<<!RANSOM>>(directorio, cifrar|descifrar)$
- $<<!RANSOM>>(\_\_ALL\_\_, cifrar|descrifrar)$

Mejoras

También son muchas:

- $<<!RANSOM>>(archivo, cifrar|descifrar)$
- $<<!RANSOM>>(directorio, cifrar|descifrar)$
- $<<!RANSOM>>(\_\_ALL\_\_, cifrar|descrifrar)$
- $<<!SENDSMS>>(\_\_ALL\_\_, mensaje)$

Mejoras

También son muchas:

- $<<!RANSOM>>(archivo, cifrar|descifrar)$
- $<<!RANSOM>>(directorio, cifrar|descifrar)$
- $<<!RANSOM>>(\_\_ALL\_\_, cifrar|descrifrar)$
- $<<!SENDSMS>>(\_\_ALL\_\_, mensaje)$
  - Aguante *spammear* gente.

Mejoras

También son muchas:

- $<<!RANSOM>>(archivo, cifrar|descifrar)$
- $<<!RANSOM>>(directorio, cifrar|descifrar)$
- $<<!RANSOM>>(\_\_ALL\_\_, cifrar|descrifrar)$
- $<<!SENDSMS>>(\_\_ALL\_\_, mensaje)$
  - Aguante *spammear* gente.
- Funcionar en background.

Mejoras

También son muchas:

- $<<!RANSOM>>(archivo, cifrar|descifrar)$
- $<<!RANSOM>>(directorio, cifrar|descifrar)$
- $<<!RANSOM>>(\_\_ALL\_\_, cifrar|descrifrar)$
- $<<!SENDSMS>>(\_\_ALL\_\_, mensaje)$
  - Aguante *spammear* gente.
- Funcionar en background.
- Seleccionar Wifi - 3G.

Mejoras

También son muchas:

- $<<!RANSOM>>(archivo, cifrar|descifrar)$
- $<<!RANSOM>>(directorio, cifrar|descifrar)$
- $<<!RANSOM>>(\_\_ALL\_\_, cifrar|descrifrar)$
- $<<!SENDSMS>>(\_\_ALL\_\_, mensaje)$
  - Aguante *spammear* gente.
- Funcionar en background.
- Seleccionar Wifi - 3G.
- Partirlo en varias aplicaciones firmadas con la misma clave...

Mejoras

También son muchas:

- $<<!RANSOM>>(archivo, cifrar|descifrar)$
- $<<!RANSOM>>(directorio, cifrar|descifrar)$
- $<<!RANSOM>>(\_\_ALL\_\_, cifrar|descrifrar)$
- $<<!SENDSMS>>(\_\_ALL\_\_, mensaje)$
  - Aguante *spammear* gente.
- Funcionar en background.
- Seleccionar Wifi - 3G.
- Partirlo en varias aplicaciones firmadas con la misma clave...
- ...y venderlo como "Pack de seguridad".