Android Malware

Francisco Arévalo
francisco.arevalo@continuum.cl

7 de agosto de 2012

Amenazas de aplicaciones

- Malware
  Software diseñado para efectuar operaciones no deseadas en un dispositivo. Puede generar cargos a la cuenta, enviar mensajes, o controlar el funcionamiento del sistema.
- Spyware
  Software que espía o recolecta datos privados sin consentimiento del usuario, incluidos e-mail, mensajes, libretas de direcciones e imágenes.
- Privacy leaks
  Aplicaciones que divulgan información privada como la ubicación, historial o aplicaciones instaladas de manera no intencional.
- Aplicaciones Vulnerabiles
  Programas con fallas de diseño, que permiten acceso no autorizado, o generan problemas con la usabilidad del dispositivo donde se instalan.

Amenazas web

- Phishing
  Páginas o formularios que suplantan o engañan al usuario para que entregue información confidencial a un atacante.
- Drive-by Downloads
  Descargas que se inician automáticamente al visitar un sitio comprometido.
- Browser exploits
  Aprovechan vulnerabilidades del explorador o sus plugins para instalar malware o ejecutar comandos en un dispositivo.

Amenazas de red

- Network exploits
  Amenazas que utilizan fallas en los protocolos de Bluetooth, Wi-Fi, SMS, o red celular para tomar control de un dispositivo.
- Sniffing Wi-Fi
  Captura de datos no ecriptados, en especial passwords y emails, al transmitirlos por una red insegura

Riesgos Físicos

- Pérdida del equipo
  El riesgo más común, ultimamente se han reportado casos de chantaje o abuso de información privada que se encuentra en un teléfono extraviado.

¿Por qué la gente instala malware?

- Repackaging

  El malware se disfraza dentro de una aplicación legítima y vuelta a publicar con un nombre e ícono similar. Ocurre a menudo con aplicaciones 'crackeadas'.
- Bait and switch

  La aplicación promete funcionalidades que en realidad no tiene, o se publica bajo una descripción falsa.
- Ataques de Update

  El autor del malware publica una aplicación legítima, pero al actualizarla, descarga una versión modificada con código malicioso.

¿Por qué la gente instala malware?

- **Shotgun distribution**

  El malware se publica bajo diversos nombres, en varios app stores, y por distintos autores. En el caso de DroidDream, se crearon más de 60 aplicaciones infectadas.

- **Malvertising**

  El desarrollador aprovecha los 'in-app advertisement' para dirigir al usuario hacia un sitio de descarga infectado. Estos avisos pueden aparecer incluso dentro de apicaciones legítimas.

- **Drive-by Downloads**

  Al visitar un sitio infectado, se inicia la descarga del malware automáticamente. Muchas veces se simulan notificaciones de 'trusted download', o diálogos para engañar al usuario y lograr que ejecute el archivo descargado.

¿Cuáles son las consecuencias?

- SMS Premium:

  GGTracker[1], RuFraud[2], aprovechan que las suscripciones a estos servicios son la forma más simple de generar cobros directamente al usuario.

- Botnets:

  DroidDream[3], convierten al equipo en un 'zombie', reciben instrucciones remotas y exponen todas las funcionalidades del teléfono (realizar llamadas, eviar mensajes, abrir conecciones a internet).

---

[1] Security Alert: Android Trojan GGTracker Charges Premium Rate SMS Messages `http://bit.ly/P3lYP6`

[2] Security Alert: Android Trojan GGTracker Charges Premium Rate SMS Messages `http://bit.ly/rTUQIu`

[3] Encyclopedia entry: TrojanSpy:AndroidOS/DroidDream.A `http://bit.ly/MKOwbL`

¿Cuáles son las consecuencias?

- Elevación de privilegios:

  Comunes al intentar 'rootear', o acceder al usuario root en un equipo. Una vez que el exploit obtiene acceso root, puede cargar aplicaciones, o acceder a cualquier funcionalidad del teléfono.

- Spyware y aplicaciones espía personalizadas:

  Pueden enfocarse a robar cualquier información que pase por el teléfono, o personalizarse para obtener credenciales bancarias o de servicios privados.

Conclusiones

- Sólo descargar aplicaciones de fuentes confiables
- Revisar que los links apunten a la dirección correcta antes de hacer click
- El buen manejo de claves y cuentas de usuario es indispensable
- Utilizar herramientas de seguridad para dispositivos móviles (Lookout, AVG, Norton, Trend Micro)
- Estar atento a comportamientos extraños en las aplicaciones, y cargos inusuales en la cuenta mensual
- Mantener el firmware actualizado
- Revisar los permisos que solicitan las aplicaciones antes de instalar

Links y contacto

- Lookout Mobile Security
  `https://www.mylookout.com/`
- Android Genome Project
  `http://lwn.net/Articles/498698/`
- IEEE Symposium on Security & Privacy
  `http://www.ieee-security.org/TC/SP2012/`

`francisco.arevalo@continuum.cl`