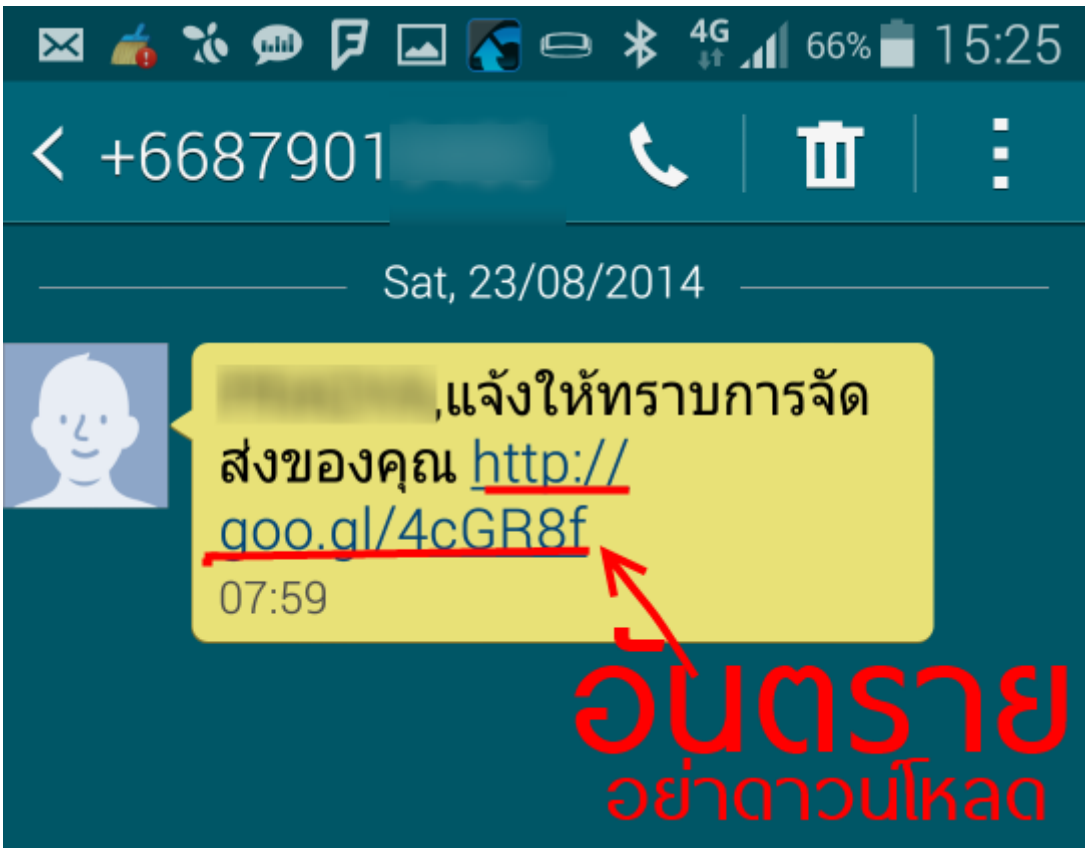
เตือนผู้ใช้ Android อย่าโหลดลิงค์ apk ใน sms ข้อความ “แจ้งให้ทราบ...”



วันนี้ประกาศเตือนถึงผู้ใช้ Android หลังทีมงาน ได้รับข้อความที่คาดว่าตอนนี้หลายๆท่านจะโดนข้อความลักษณะนี้ คือ ” (ชื่อเรา), แจ้งให้ทราบการจัดส่งของคุณ [ลิงค์ดาวน์โหลด]“ ในข้อความ sms ซึ่งลิงค์นั้นเป็นลิงค์เข้าสู่การดาวน์โหลดไฟล์ apk ที่มีมัลแวร์ซ่อนอยู่ ย้ำอย่าดาวน์โหลดเด็ดขาด

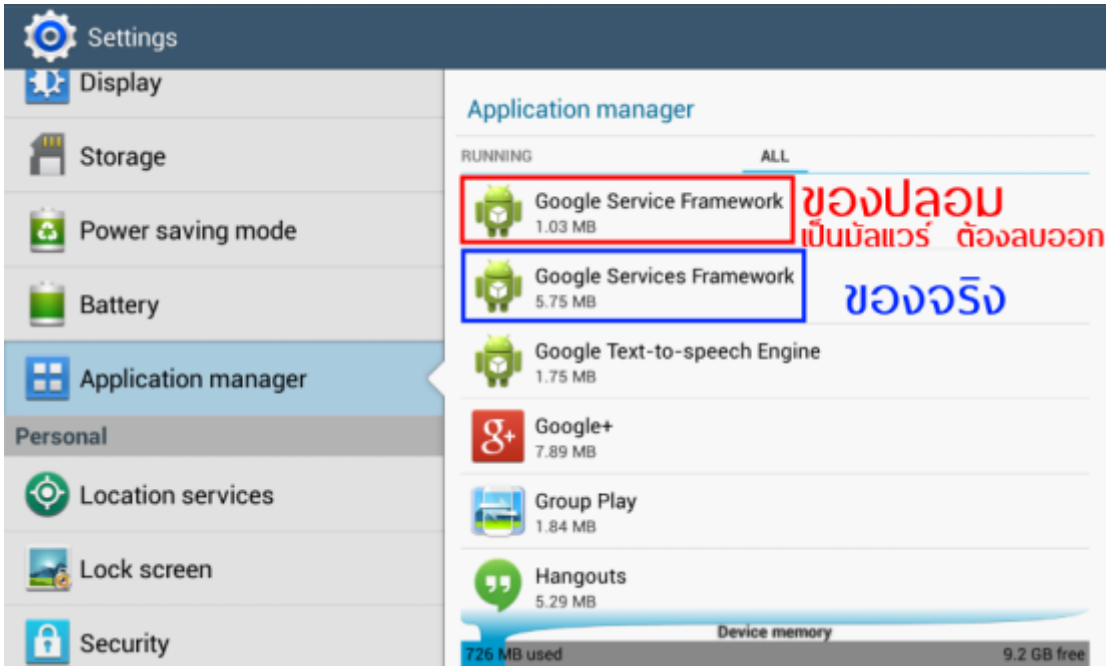
มัน อันตรายแค่ไหน ? ทางหน่วยงานด้านความปลอดภัย Thaicert ได้ให้รายละเอียดในเว็บไซต์ว่า ไฟล์ลิงค์ใน sms “แจ้งให้ทราบการจัดส่งของคุณ” ว่า จากการตรวจสอบข้อมูลไฟล์ .apk ดังกล่าวด้วยใช้เว็บไซต์ Virustotal พบว่าเป็นโทรจันที่มีความสามารถในการขโมยข้อมูล SMS เป็นหลัก ซึ่งมีลักษณะที่คล้ายกับมัลแวร์ที่มีเป้าหมายเพื่อโจมตีผู้ใช้งานระบบธุรก รรมออนไลน์ต่างๆ เช่น e-Banking ด้วยการขโมย SMS มาใช้ในการทำธุรกรรมออนไลน์ ตามที่เคยเกิดขึ้นมาแล้วในอดีต

และเมื่อมีการนำไฟล์มัลแวร์ทั้งหมดมาทำการ Decompile **พบว่าซอร์สโค้ดของไฟล์มัลแวร์ แจ้ง.apk และ ไฟล์มัลแวร์ รับทราบ.apk มีการทำงานเหมือนกันทุกประการ เพียงแค่เปลี่ยนชื่อไฟล์ให้ไม่เหมือนกันเทานั้น** โดยมัลแวร์ตัวที่ว่านี้จะอ่านอ่านรายชื่อเบอร์โทรศัพท์ อ่าน แก้ไข และรับส่งข้อความ SMS รวมถึงเชื่อมต่ออินเทอร์เน็ต

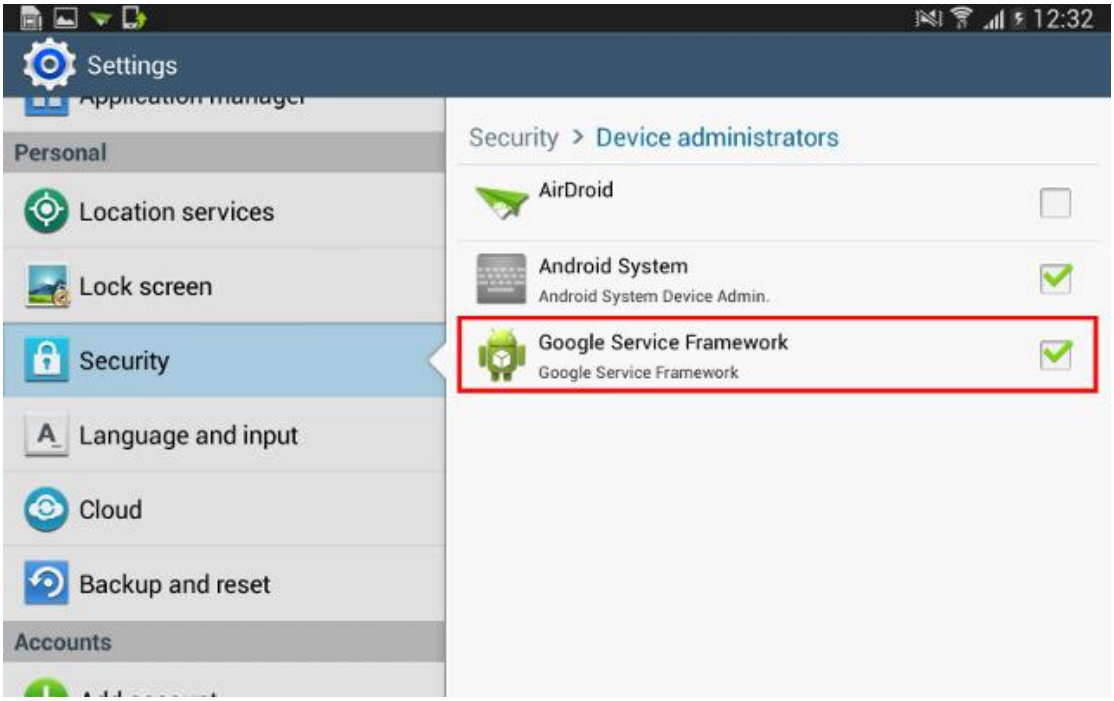
โดยหลักการทำงานของไฟล์ APK ใน sms อันตรายนี้ หาก ติดตั้งลงในเครื่อง แอปพลิเคชันลักลอบส่ง SMS ออกไปยังหมายเลขโทรศัพท์อื่นๆ ที่ถูกบันทึกอยู่ในเครื่อง เพื่อแพร่กระจายมัลแวร์ไปยังผู้ใช้รายอื่น สามารถขโมยข้อมูล หรือทำให้ผู้ที่ติดตั้งแอปพลิเคชันดังกล่าวเสียเงินค่าส่ง SMS เป็นจำนวนมากได้ นอกจากนี้ ไฟล์ apk อันตรายใน sms นี้ยังมีการร้องขอสิทธิ์ Device administration ในการล็อกหน้าจอ ซึ่งอาจมีจุดประสงค์ที่ไม่ดีอื่น ๆ ด้วย

โดยการออกแบบครั้งนี้หวังโจมตีเหยื่อที่หลงเชื่อข้อความ sms บนระบบปฏิบัติการ Android เพราะ ไฟล์ apk รันได้เฉพาะ Android เท่านั้น

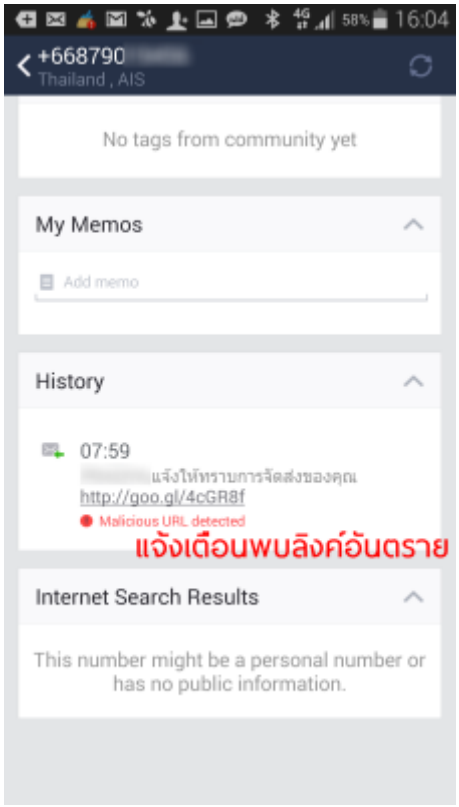
วิธีแก้ไขสำหรับคนที่เผลอติดตั้ง ไฟล์ apk จาก sms อันตรายแล้ว



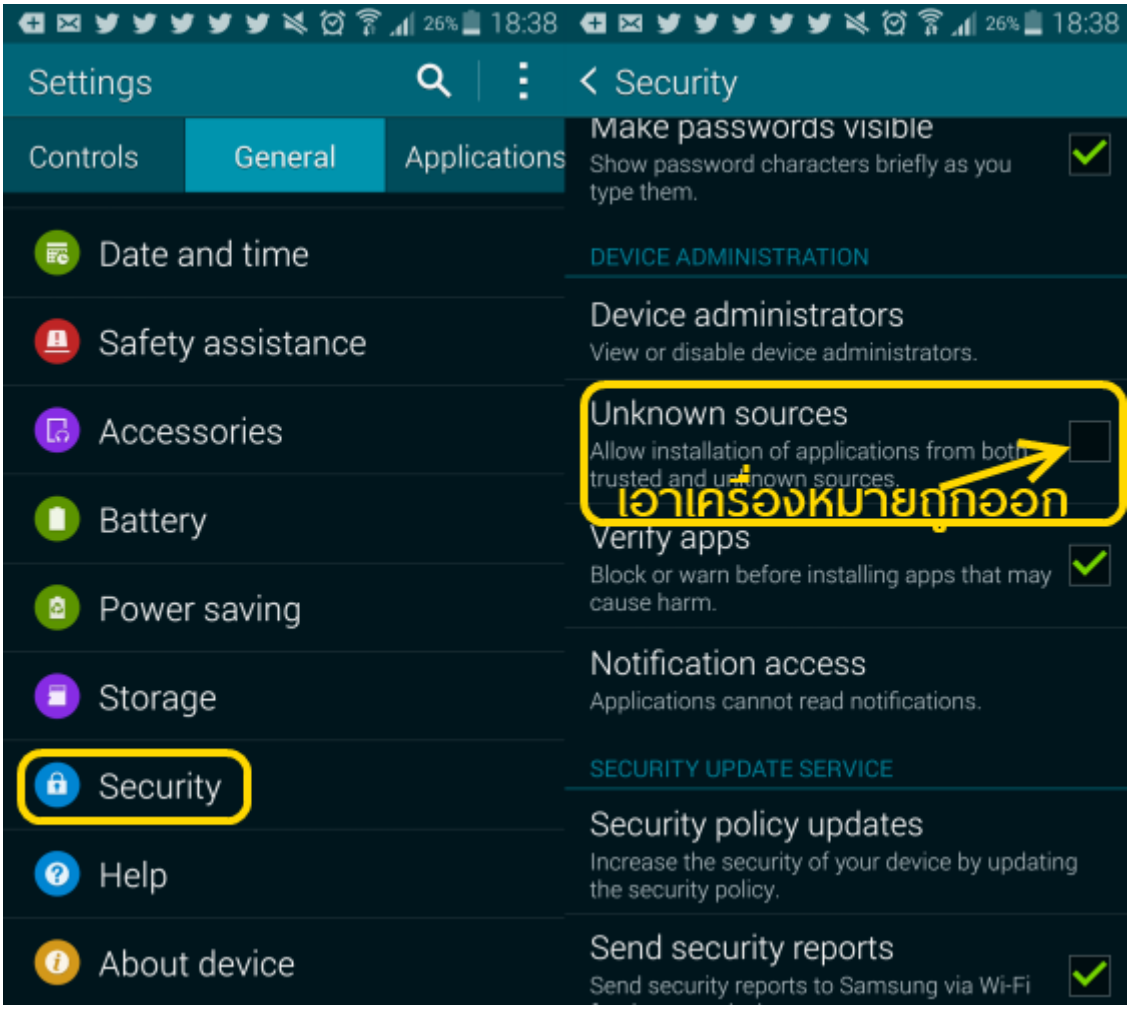
หากคุณติดตั้ง apk ลงเครื่องแล้ว แอปอันตรายนี้จะใช้ชื่อว่า **Google Service Framework** ซึ่งตั้งชื่อคล้ายคลึงกับแอปพลิเคชันจริงที่ชื่อว่า Google Services Framework (สังเกตของจริงแท้ ต้องมีs ต่อท้าย Service) ดังนั้นสำหรับผู้ใช้งานที่ติดตั้งแอปพลิเคชันดังกล่าวไปแล้ว ให้รีบถอนแอปที่ติดไปนี้ออก



โดยเข้าไปที่ **Settings > Security > Device administrators** แล้ว**ติ๊กเครื่องหมายถูกออกหลังแอป Google Service Framework** ตามรูปข้างบน ตรงสีแดงนี้ เพื่อถอนการให้สิทธิ์ Device administration จากนั้นให้ถอนการติดตั้งแอปพลิเคชันตามขั้นตอนปกติ



สำหรับ รายละเอียดเพิ่มเติมเกี่ยวกับข้อมูลมัลแวร์นี้อย่างเจาะลึก สามารถดูได้ที่เว็บไซต์ Thaicert ทั้งนี้ผู้ใช้สมาร์ทโฟนหากเจอข้อความแปลกๆพร้อมลิงค์ำอย่าคลิกอย่าแตะลิงค์เด็ดขาด และควรตรวจสอบด้วยการติดตั้งซอฟต์แวร์ Antivirus บนมือถือคุณด้วย ซึ่งตัวอย่างนี้ แอพ **Line Whos Call** สามารถรายงานผลว่าลิงค์ที่แนบมาใน sms ว่า เป็นลิงค์อันตรายด้วย ดังนั้นควรติดตั้งโปรแกรม Antivirus เพื่อความปลอดภัยต่อข้อมูลของโทรศัพท์ของคุณ



และวิธีป้องกันอีกวิธีนึง คือ ให้เข้าไปที่ **settings** >> เลือก **Security** แล้ว สังเกตที่ **Unknow sources ว่ามีติ๊กถูกหรือไม่ ถ้ามี...ให้ติ๊กเอาเครื่องหมายถูกออกไป!!!** เพื่อไม่ให้ทำการรันไฟล์ apk บนเครื่อง Android ของคุณได้ และวิธีนี้จะช่วยให้สมาร์ทโฟนของคุณปลอดภัยขึ้นด้วย

ข้อมูลจาก Thaicert

ที่มา : http://www.it24hrs.com/2014/sms-apk-danger/