

BAB V PENUTUP

5.1 Kesimpulan

1. Berikut kesimpulan yang dapat ditarik dari pembahasan dalam tugas akhir ini:
 - a. Tahapan untuk melakukan analisis *statis* menggunakan reverse engineering pada aplikasi *syssecApp.apk* yaitu sebagai berikut :
 - b. Mengidentifikasi sample aplikasi *syssecApp.apk* menggunakan *Virus total*. Ditemukan bahwa aplikasi tersebut teridentifikasi 26 *antimalware* dari 64.
 - c. Menghitung *checksum* (hashing) aplikasi. Didapatkan hasil SHA 256 aplikasi *syssecApp.apk* yaitu “f01dd91e61d8e8047599d9cea20e15f77980c1cdd4c17743ab55b17eb9c42be3”
 - d. Melakukan *Decompile* aplikasi menggunakan *Apktool* dan didapatkan hasil data aplikasi seperti *certificate*, *source*, *Smali* dan *AndroidManifest.xml*
 - e. Memasukkan analisis *permission* pada aplikasi *syssecApp.apk* dan ditemukan 13 *permission* pada aplikasi tersebut.
 - f. Melakukan analisis *source code* pada aplikasi *syssecApp.apk* menggunakan *tools JD-GUI* dan ditemukan 1 *class* yang berfungsi untuk mengirim *file data* ke *host (127.0.0.1)* merupakan *localhost* bukan *Ip Publik* milik *attacker*.
2. Analisis *dinamis* yang dilakukan pada *emulator Genymotion* dengan diberi hak akses *full* dan berhasil mendapatkan *class* yang berisi *sentHost (127.0.0.1)*,

5.2 Saran

Penulis penelitian skripsi ini berharap informasi yang diberikan dapat bermanfaat bagi penulis, pembaca, dan pengguna aplikasi Android dalam berbagai cara pada akhirnya. Penulis sangat menyadari keterbatasan

metode rekayasa balik untuk menganalisis malware Trojan. Oleh karena itu, penulis dapat memberikan saran sebagai berikut:

- a. Penelitian tentang malware sangatlah luas. Teknik deteksi malware mencakup berbasis perilaku, pembelajaran mendalam, deteksi basis tanda tangan, dan rekayasa balik.
- b. Untuk penelitian selanjutnya, dapat dititik fokuskan dalam pembuatan *antiVirus* sederhana dalam mencegah *malware Trojan*.
- c. Pengguna Android harus mengunduh aplikasi dari situs web terkemuka (Google Playstore), dan sebelum menginstal aplikasi, mereka harus terlebih dahulu memeriksa izin akses aplikasi dengan antivirus untuk melihat apakah aplikasi tersebut mengandung malware.
- d. Penulis menyarankan pengguna Android untuk menonaktifkan penginstalan perangkat lunak pihak ketiga di pengaturan perangkat. Dengan mencoba meniru pembaruan sistem dan proses serupa lainnya, ini menghilangkan ancaman yang diunduh secara acak. Hapus centang atau nonaktifkan kotak berlabel "Sumber Tidak Dikenal" (Unknown Sources) di pengaturan Android.