BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pembahasan penelitian dalam skripsi ini, maka dapat diambil kesimpulan sebagai berikut:

1. Tahapan untuk melakukan analisis statis menggunakan *reverse engineering* pada aplikasi kamus kesehatan yaitu sebagai berikut :
   a. Mengidentifikasi *sample* aplikasi kamus kesehatan dengan menggunakan *Virus Total*. Ditemukan bahwa aplikasi tersebut terindentifikasi 17 dari 62 *antimalware* dengan 3 *antimalware* mengkategorikan sebagai *malware trojan downloader*.
   b. Menghitung *Checksum (hashing)* aplikasi. Didapatkan nilai *hashing SHA 256* aplikasi kamus kesehatan yaitu *"aafcd5c804d32961c3dac901a7926797a44ef4ae255bb30a6d812b00e843eea7"*.
   c. Melakukan d*ecompiler* aplikasi menggunakan *MARA Framework* dan didapatkan hasil data aplikasi seperti *certificate, source, smali* dan *AndroidManifest.xml*
   d. Melakukan analisis *permissions* pada aplikasi kamus kesehatan dan ditemukan 27 *permissions* pada aplikasi tersebut.
   e. Melakukan analisis *source code* pada aplikasi kamus kesehatan menggunakan *tools JD-GUI* dan ditemukan 1 folder yang bersifat *malicious* yaitu folder *"edyhw"*. Folder *"edyhw"* berisi 8 *class* yaitu *"Iejxi.class, Mxedd.class, Tamdj.class, a.class, b.class, c.class, d.class, e.class, f.class, dan g.class."*
   f. Melakukan pemetaaan *TTP* dengan model *Mitre ATT&CK*. Didapatkan data bahwa *malware trojan malware* yang menyisipi

aplikasi kamus kesehatan memberikan *impact* berbahaya yaitu penyerang mendapatkan hak akses penuh yang dapat digunakan untuk *delete devices data* dan *carrier billing fraud*.

2. Dari analisis dinamis yang dilakukan pada *devices Samsung Galaxy S10* menggunakan *genymotion android emulator* terdapat perbedaan pada proses hak akses perizinan, dimana aplikasi kamus kesehatan yang telah terinfeksi *malware trojan downloader* memiliki 8 hak akses perizinan yaitu *call logs, camera, contacts, location, microphone, phone, sms,* dan *storage*.

3. Hasil perbandingan analisis aplikasi kamus kesehatan sebelum dan sesudah terinfeksi *malware trojan downloader* adalah sebagai berikut :

   a. Dari analisis statis menggunakan *MobSF* ditemukan perbedaan ukuran file pada aplikasi kamus kesehatan. Dimana setelah *ter-embedded malware*, ukuran file menjadi 10.17 MB yang sebelumnya adalah 10.05 MB. Tentunya dengan perubahan ukuran file, maka secara otomatis juga perubahan pada *hashing SHA256*.

   b. *MobSF* menemukan adanya perubahan pada *permissions* yang sebelumnya hanya ada 9 *permissions*, namun setelah *ter-embedded malware* ditemukan 18 *permissions* tambahan sehingga total keseluruhan menjadi 27 *permissions*.

   c. *MobSF* menemukan penghapusan *fingerprint* pada aplikasi kamus kesehatan yang terinfeksi *malware trojan downloader*.

   d. *MobSF* menemukan adanya perubahan pada *services* yang sebelumnya hanya ada 5 *services*, namun setelah terinfeksi *malware trojan downloader* ditemukan 6 *services*.

   e. *MobSF* menemukan adanya perubahan pada *receivers* yang sebelumnya hanya ada 3 *receivers*, namun setelah terinfeksi *malware trojan downloader* ditemukan 4 *receivers*.

4. Berhasil dalam mengimplementasikan teknik analisis dinamis dengan uji hasil kerja *malware trojan downloader*, yaitu berhasil menjalankan 8 perintah seperti *sysinfo, ifconfig, app_list, play, screenshot, dump_calllog, dump_sms,* dan *send_sms.*

5.2 Saran

Sebagai penutup penelitian skripsi ini, penulis berharap semoga apa yang penulis sajikan dapat memberikan banyak manfaat bagi pembaca, penulis dan pengguna aplikasi *android.*

Penulis menyadari sepenuhnya bahwa analisis *malware trojan downloader* menggunakan metode *reverse engineering* ini masih memiliki kekurangan, oleh karena itu saran yang dapat penulis berikan antara lain:

1. Malware adalah topik penelitian yang masih sangat terbuka luas. Selain memanfaatkan *reverse engineering*, deteksi *malware* dapat dilakukan pula menggunakan *signature base detection, behaviour based, deep learning.*
2. Untuk penelitian selanjutnya, dapat dititik fokuskan dalam pembuatan *antivirus* sederhana dalam mencegah *malware trojan downloader.*
3. Bagi para pengguna *android* sebaiknya mendownload aplikasi *android* dari situs terpercaya *(Google playstore),* dan sebelum memutuskan menginstal aplikasi sebaiknya memeriksa terlebih dahulu dengan *anti virus* apakah aplikasi tersebut mengandung *malware*, serta terlebih dahulu memeriksa izin akses yang dijalankan oleh aplikasi.
4. Penulis menyarankan pengguna *android* memblokir instalasi perangkat lunak dari sumber pihak ketiga dalam pengaturan perangkat. Ini menghilangkan ancaman yang diunduh secara acak dengan upaya meniru pembaruan sistem dan sejenisnya. Bukalah pengaturan *android* anda, kemudian pilih Keamanan dan hapus centang/non-aktifkan kotak 'Sumber Tidak Dikenal' *(Unknown Sources).*