BAB V
PENUTUP

5.1 Kesimpulan

Setelah penelitian dilakukan, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Identifikasi *sample malware* gandcrab ransomware dengan menggunakan virustotal. Ditemukan *sample malware* tersebut teridentifikasi 60 dari 70 *antimalware* dengan 13 *antimalware* mengkategorikan sebagai *ransomware*.
2. Didapatkan nilai *hashing* SHA26 dari *sample malware* gandcrab *ransomware* yaitu "49b769536224f160b6087dc866edf6445531c6136ab76b9d5079ce622b043200".
3. Melakukan pencarian *strings* dan berhasil menemukan beberapa fungsi *strings* yang berupa fungsi DLL. Adapun fungsi DLL yang diakses oleh *sample malware* gandcrab ialah MFC42.DLL, MSVCRT.DLL, KERNEL32.DLL, USER32.DLL, GDI32.DLL, ADVAPI32.DLL, dan SHELL32.DLL.
4. Melakukan analisa dari setiap fungsi *strings* dan mendapatkan karakteristik juga cara kerja dari *sample malware* gandcrab ransomware.
5. Malware gandcrab ransomware sangat berbahaya karena mampu mengakses dara pribadi dari pengguna dan mengunci data tersebut.

5.2 Saran

Dalam melakukan penelitian ini, peneliti sadar masih banyak kekurangan. Sehingga, penulis memberikan saran-saran yang dapat dilakukan untuk penelitian kedepannya. Diantaranya adalah:

Sehingga, penulis memberikan saran-saran yang dapat dilakukan untuk penelitian kedepannya. Diantaranya adalah:

1. Menggunakan lebih banyak *tools* analisis *malware* agar penelitian lebih maksimal.
2. Melakukan *debugger* dan *disassembler* untuk penelitian selanjutnya.
3. Melakukan analisis dinamis *malware* gandcrab ransomware.
4. Penelitan selanjutnya, dapat dititik fokuskan dalam pembuatan antivirus yang dapat mencegah malware gandcrab ransomware ini.
5. Mengikuti perkembangan dan trend malware yang sedang terjadi. Karena, seiring berkembangnya teknologi, maka perkebangan kejahatan siber juga akan semakin canggih.