BAB V

PENUTUP

5.1 Kesimpulan

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

1. Hasil perbandingan menunjukkan sebuah perbedaan antara voidcrypt yaitu *crypto ransomware* dan virlock yaitu *locker ransomware* dalam mengunci dan lamanya process ketika dijalankan. Hasil menunjukkan bahwa dalam process lebih cepat virlock yaitu jenis *locker ransomware* dan voidcrypt cenderung lebih lama dalam menginfeksi sebuah *file*.
2. Hasil perbandingan pada segi sistem voidcrypt dapat mengenkripsi seluruh *file* baik video, music ataupun dokumen yang berada di dalam suatu OS yang penulis jalankan di *windows* 10. Untuk virlock *ransomware* menunjukkan *file* masih utuh dan dapat dibuka dalam waktu beberapa detik. Akan tetapi setelah itu tampilan akan Kembali ke tampilan dimana terdapat tampilan dari virlock itu sendiri.
3. Hasil yang ditunjukkan voidcrypt *ransomware* pada tabel TTPs pada web analyze diperlihatkan voidcrypt *ransomware* dapat memodifikasi atau menghapus kunci refistry atau *file* konfigurasi sehingga perangkat tidak beroperasi dengan benar
4. Hasil yang ditunjukkan virlock *ransomware* pada tabel TTPs pada web analyze diperlihatkan hacker atau penjahat dapat membentuk perilaku tindak lanjut, termasuk dapat menginfeksi target sepenuhnya.
5. Hasil perbandingan pada *virus total* menunjukkan bahwa hasil virlock *ransomware* memiliki engine lebih besar daripada *crypto ransomware* dengan hasil 62/69 dari *antivirus* yang disediakan oleh *virus total*. Sedangkan pada hasil laporan untuk voidcrypt *ransomware* menunjukkan hasil 49/69 dari *antivirus* yang disediakan oleh *virus total*.

5.2 Saran

Sebagai penutup penelitian skr*ip*si ini, penulis berharap semoga apa yang penulis sajikan dapat memberikan banyak manfaat bagi pembaca, penulis dan pengguna *windows* agar

penulis menyadari sepenuhnya bahwa analisis *ransomware crypto* dan *locker* menggunakan metode dynamic analyze ini masih memliki kekuranganm oleh karena itu saran yang dapat penulis berikan antara lain:

1. *Ransomware* merupakan sebuah *malware* yang sangat berbahaya dan merugikan banyak pihak. Untuk melakukan analisa sebuah *malware* atau *ransomware* di*p*erlukan beberapa kali penelitian dan tools-tools yang dapat membantu untuk mencari informasi agar bisa didapat sebuah informasi yang lebih lengkap.
2. Bagi para pengguna *windows* disarankan agar lebih berhati-hati dalam mendapatkan sebuah email atau mengakses situs-situs yang mencurigakan untuk menghindari phising yang akan mengambil alih dengan cara meremote perangkat tersebut untuk mendapatkan berbagai informasi. Setelah didapat informasi tersebut seorang hacker akan mengambil alih perangkat tersebut lalu mematikan *windows* defender agar *ransomware* dapat dijalankan.
3. Untuk penelitian selanjutnya, selalu update tentang jenis *ransomware* atau *malware* agar dapat diketahui informasi sifat dan efek yang terjadi apabila menyerang atau menginfeksi suatu sistem pada computer.