DAFTAR GAMBAR

Gambar 2.1 Format *File* PE (Saxe dan Sanders, 2018) II-10

Gambar 3.1 Tahapan Penelitian III-1

Gambar 4.1 Pengunduhan *sample malware* IV-2

Gambar 4.2 Sampel *Malware* IV-3

Gambar 4.3 Nilai *Hash Sample Malware* IV-3

Gambar 4.4 Deteksi jenis *file sample malware* IV-4

Gambar 4.5 *Flowchart static analysis* IV-5

Gambar 4.6 *strings extract* IV-6

Gambar 4.7 hasil *decompile* IV-7

Gambar 4.8 Obfuscation Detect IV-8

Gambar 4.9 *Deobfuscate* menggunakan *de4dot* IV-8

Gambar 4.10 *Obfuscation Detect* ke-2 ..... IV-9

Gambar 4.11 *flowchart dynamic analysis* IV-10

Gambar 4.12 *process monitoring* setelah *malware* dijalankan IV-11

Gambar 4.13 *vbc.exe child process tree* IV-11

Gambar 4.14 *vbc.exe* melakukan aktivitas *network* IV-12

Gambar 4.15 *malware* melakukan koneksi ke 37.220.87.47 ..... IV-13

Gambar 4.16 *Malware Workflow* IV-16