ABSTRAK

Era serba digital saat ini, data menjadi sebuah aset yang sangat berharga. Berbagai macam teknik digunakan untuk mencuri data pribadi yang berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab. Objek yang digunakan pada penelitian ini adalah *AQUVAPRN.exe* yang memiliki jenis *malware RAT* (*Remote Access Trojan*) yang saat *malware* ini berjalan pembuat *malware* tersebut dapat mengambil data pribadi pengguna yang sistem operasinya terinfeksi. Cara kerja dari *malware AQUVAPRN.exe* dengan berjalan pada latar belakang saat aplikasi dijalankan atau dieksekusi lalu membuat beberapa proses seperti menginfeksi 36 *file registry*, membuat 65 *file*, membaca 52 *file* pada sistem operasi yang terinfeksi, dan melakukan koneksi internet dengan *IP Address* tertentu secara terus menerus tanpa diketahui oleh pengguna dari komputer itu sendiri. Hasil yang diperoleh terhadap *malware AQUVAPRN.exe* berupa alamat *IP Address* 109.51.76.80, memiliki domain Kota Lisbon Negara Portugal, memiliki nilai *hash* MD5 `55c2c12970cda52f58bfad7b8c7d37d5`. Diketahui pula, *malware AQUVAPRN.exe* menggunakan teknik *anti reverse engineering* tepatnya *obfuscation* yang menghambat atau menghalangi *malware* untuk dibedah atau di *reverse engineering* agar mengetahui *code* penyusun dari *malware*. Hasil *PID* dari proses *AQUVAPRN.exe* pada sistem operasi yang terinfeksi adalah 8332 dengan alat virtual (*Virtual Address*) `0x8e0f57042080`.

Kata Kunci: Data Pribadi, *IP Address*, *Malware*, *Obfuscation*, *RAT*