ABSTRAK

Malware adalah sebuah perangkat lunak atau yang diciptakan untuk melakukan penyusupan atau melakukan perusakan pada sistem komputer. Untuk penyebaran *malware* saat ini begitu mudah baik melalui *flashdisk*, iklan-iklan tertentu pada *website*, dan media lainnya. Semuanya sangat erat kaitannya dengan tindak kejahatan seperti pencurian *file*, kartu kredit, *internet banking* dan lain sebagainya. Salah satu *malware* yang dapat mengendalikan komputer pengguna secara diam-diam dan dari jarak yang jauh adalah *malware poison ivy*, dikenal sebagai "*Remote Acces Trojan*" karena dapat memberikan kontrol penuh melalui pintu belakang (*backdoor*).

Pada proyek tingkat ini malware Poison Ivy akan di analisa untuk mengetahui cara kerja dari malware Poison ivy tersebut, Analisa dilakukan dengan metode analisis statis dan dinamis dimana kombinasi dari metoda tersebut merupakan kombinasi yang sesuai untuk menganalisa cara kerja dari sebuah malware.

Berdasarkan Analisa ini Malware Poison Ivy bekerja dengan cara menginject file dll yaitu loadlibrary.dll untuk mengontrol system pada computer target lalu penambahan file dan registry pada komputer target dan saat server melakukan koneksi dengan komputer target lalu sebelum melakukan koneksi malware poison ivy melakukan proses pencocokan password dan jika password cocok maka komputer server dapat mengakses komputer target. Dan malware poison ivy tidak memakan terlalu banyak resource pada sebuah system computer.

***Keywords*:** *Poison ivy, Remote Access Trojan(RAT), Malware.*