ABSTRAK

Redline Stealer adalah *variant malware* yang ditemukan pada awal Maret 2020 oleh analis *proofpoint*. *Redline Stealer* terkenal dengan kemampuannya yang dapat menghindari deteksi *antivirus*. *Redline Stealer* dibuat oleh *hacker* dengan tujuan untuk mencuri informasi sensitif korban seperti informasi data *username, password* dan kartu kredit dari aplikasi *browser* yang digunakan komputer korban. Penelitian ini menggunakan metode analisis *static* dan *dynamic* untuk proses analisis *Redline Stealer*. Proses analisis *static* dilakukan dengan cara melakukan pengamatan terhadap *file sample malware,* sedangkan analisis *dynamic* dilakukan dengan cara memantau aktivitas *malware* saat *malware* dijalankan pada sistem. Hasil analisis menunjukkan bahwa *malware Redline Stealer* ini menggunakan fitur *obfuscation*, berbasis *.net*, hanya aktif ketika terdapat koneksi, mencuri informasi sensitif terutama pada aplikasi *browser. Malware* tersebut menjalankan proses *vbc.exe* dan mengirimkan informasi yang berhasil dicuri melalui *vbc.exe* ke server *malware* yang beralamat ip 37.220.87.47. Penanganan yang pada komputer yang sudah terinfeksi oleh *malware Redline Stealer* adalah dengan cara memblokir ip 37.220.87.47, mengentikan proses *vbc.exe* pada *task manager* serta menghapus file *malware* dan *vbc.exe*.

***Kata kunci*:** Analisis *Malware, Obfuscation, Redline Stealer*