# ABSTRAK

Perkembangan teknologi informasi yang pesat tidak hanya memberikan kemudahan bagi pengguna, tetapi juga memunculkan berbagai ancaman keamanan siber seperti penyebaran *malware*. Salah satu jenis *malware* yang berbahaya adalah *Remote Access Trojan (RAT),* yaitu *malware* yang memungkinkan penyerang untuk mengendalikan sistem korban dari jarak jauh tanpa sepengetahuan pengguna. Penelitian ini bertujuan untuk menganalisis perilaku *malware* ramez.exe dengan menggunakan metode *Memory Forensics* dan *YARA Rules*, guna mengetahui karakteristik, aktivitas, serta pola kerja *malware* secara menyeluruh. Metode penelitian yang digunakan adalah pendekatan kualitatif deskriptif, dengan melakukan analisis forensik digital terhadap sampel *malware* menggunakan dua tahapan utama, yaitu analisis memori (*runtime analysis*) dengan *Volatility Framework*, dan analisis menggunakan *YARA Rules*. Proses analisis dilakukan berdasarkan 16 parameter penelitian yang mencakup aktivitas proses, koneksi jaringan, *registry*, artefak *file*, *string* unik, domain eksternal, serta struktur internal *malware*. Hasil penelitian menunjukkan bahwa *malware* ramez.exe berfungsi sebagai *dropper* yang mengeksekusi *payload* remcos.exe, berjalan di latar belakang sistem operasi, serta melakukan koneksi ke alamat IP 147.185.221.26:40252 yang berlokasi di Carson, Amerika Serikat. Berdasarkan hasil analisis *Memory Forensics*, ditemukan aktivitas proses berbahaya seperti injeksi ke sistem, pembuatan *child process*, modifikasi *registry*, dan upaya persistensi agar *malware* tetap aktif setelah sistem *direstart*. Sedangkan hasil analisis YARA Rules berhasil mendeteksi *string* dan pola penting seperti rmclient.exe, sysinfo.txt, dxdiag, cmd.exe, image/jpeg, serta http://geoplugin.net/json.gp, yang menunjukkan kemampuan *malware* untuk mengumpulkan informasi sistem korban, mengeksekusi perintah jarak jauh, dan melakukan komunikasi tersembunyi dengan server eksternal. Berdasarkan keseluruhan hasil, dapat disimpulkan bahwa metode *Memory Forensics* dan *YARA Rules* saling melengkapi dalam proses analisis malware. *Memory Forensics* efektif untuk mendeteksi artefak dinamis yang terjadi di dalam memori, sedangkan *YARA Rules* unggul dalam mengidentifikasi artefak statis dan struktur internal *file*. Kombinasi kedua metode tersebut menghasilkan analisis yang komprehensif dan mendalam terhadap perilaku *malware* ramez.exe yang dikategorikan sebagai *Remote Access Trojan (RAT).*

**Kata Kunci:** *Memory Forensics, YARA Rules, Malware, ramez.exe, Remote Access Trojan (RAT).*