

ABSTRAK

Domain Generation Algorithms (DGAs) secara otomatis menghasilkan sejumlah besar nama domain *pseudo-random* untuk komunikasi *command-and-control* (C2), sehingga menimbulkan tantangan signifikan bagi mekanisme keamanan jaringan. Meskipun detektor berbasis *machine learning* telah menunjukkan akurasi tinggi untuk DGA yang terwakili dalam data pelatihan, hanya 26% dari penelitian sebelumnya yang secara eksplisit mengevaluasi *generalisasi lintas-keluarga*, dan performa model seringkali menurun ketika menghadapi keluarga DGA yang belum pernah dilihat sebelumnya. Untuk mengatasi hal ini, kami mengembangkan pengklasifikasi *Random Forest* yang menggunakan *skema pelatihan split-ensemble*, terdiri dari 24 *sub-ensemble terstratifikasi* yang diintegrasikan melalui *majority voting*. Model ini mengandalkan 12 fitur tingkat domain, yang mencakup karakteristik berbasis *entropi*, struktural, linguistik, dan sekuensial. Evaluasi eksperimental dilakukan pada 120 keluarga DGA, di mana 65 keluarga secara ketat tidak diikutsertakan dalam fase pelatihan untuk mengemulasi skenario *zero-day* yang realistis. Model *split-ensemble* yang diusulkan mencapai *Matthews Correlation Coefficient* (MCC) sebesar 0,965 (95% CI: 0,963–0,967) pada keluarga *zero-day* tersebut, dengan seluruh 65 keluarga yang ditahan melampaui ambang batas generalisasi $MCC = 0,70$. Fitur terkait *entropi* menyumbang 60,2% dari *feature importance* teragregasi dan menunjukkan peringkat relatif yang stabil di seluruh pengaturan evaluasi (Spearman's $\rho = 1,0$). Strategi *pelatihan split-ensemble* mengurangi degradasi performa akibat *distribution shift* sebesar 73% relatif terhadap *baseline model tunggal* ($\Delta MCC = 0,095$, $p < 0,001$). *False positive rate* yang dihasilkan sebesar 0,17% berada dalam rentang yang dapat diterima untuk penerapan operasional. Secara keseluruhan, temuan ini mengindikasikan bahwa keragaman dalam proses pelatihan, bukan peningkatan kompleksitas arsitektur, merupakan faktor utama yang menentukan generalisasi terhadap keluarga DGA *zero-day*. Dengan demikian, model *ensemble* yang ringan dan dapat diinterpretasikan mampu mencapai performa *deteksi zero-day* yang kompetitif, menawarkan alternatif yang efisien secara sumber daya dan transparan secara operasional dibandingkan metode berbasis *deep learning*, sehingga sangat cocok untuk diintegrasikan ke dalam alur kerja *Security Operations Center*.

Kata Kunci: *Domain Generation Algorithm, deteksi zero-day, machine learning, ensemble Random Forest, keamanan siber, deteksi malware*