Pengembangan metode ekstraksi kode tersembunyi berbasis flux dari packed binary executable untuk meningkatkan pemahaman perilaku malicious code = Development of flux-based hidden code extraction method from packed binary executable for improved comprehension of malmalicious
code behavior

Charles Lim, author

Abstrak

ABSTRAK
Pengemas kode biner umumnya digunakan untuk melindungi kode asli di dalam kode biner yang dapat dieksekusi sehingga terdeteksi sebagai kode berbahaya oleh perangkat lunak anti-malware. Berbagai metode unpacking packed binary executable telah dipelajari secara ekstensif, beberapa pendekatan unpacking telah diajukan. Beberapa solusi ini tergantung pada berbagai asumsi, yang dapat membatasi keefektifannya. Metode baru teknik analisis memori berbasis flux diusulkan untuk menentukan akhir fungsi pembongkaran untuk memungkinkan ekstraksi kode tersembunyi dari kode biner yang dapat dikemas. Hasil penelitian menunjukkan bahwa metode kami memberikan kinerja yang lebih baik daripada metoda sebelumnya dalam mengekstrak kode tersembunyi dari packed binary executable. Khususnya pada packed benign executable menghasilkan nilai similarity rata-rata mencapai 92% bila dibandingkan dengan benign executable original sedangkan 70% sampel malware berhasil diekstraksi dan terdeteksi sebagai unpacked.
<hr><i>ABSTRACT
Binary packer has been commonly used to protect the original code inside the binary executables being detected as malicious code by anti-malware software. Various methods of unpacking packed binary executables have been extensively studied, several unpacking approaches have been proposed. Some of these solutions depends on various assumptions, which may limit their effectiveness. A new method of flux-based memory analysis technique is proposed to determine the end of unpacking routine to allow hidden code extraction from the packed binary executables. Our experiments show that our method provides better performance than previous works in extracting the hidden code from the packed binary executable. In particular, experiments on packed benign executable exhibit an average of 92% on similarity compared with the original benign executable while 70% of extracted hidden code from malware samples detected as unpacked.