Analisis varian dan tren malware menggunakan metode analisa dinamis dan forecasting berbasis algoritma time series = The varians and trend of malware analysis using dynamic analysis and forecasting method with time series algorithm

Yopi Fakhruzi, author

Abstrak

Penelitian ini membahas tentang penelitian terhadap sekelompok data laporan anomali trafik internet Indonesia oleh badan ID-SIRTII sebagai lembaga CSIRT (Computer Science Incident Response Team) Indonesia. Menganalisis cara mengenal varian malware yang sedang berkembang beserta signature, behavior, dan impact masing-masingnya menggunakan Metode analisa dinamis dengan web-based tools sebagai media pendukung. Melakukan analisis forecasting berbasis algoritma time series untuk mengetahui tren malware beserta prediksinya. Trafik internet Indonesia memiliki 21 kategori anomali terbesar dengan total 39.121.466 serangan selama tahun 2012, dimana 54% terdiri dari jenis serangan SQL dan 15% terdiri dari jenis serangan Botnet. Diprediksikan jenis network incident oleh Worm akan terus berkembang selama tahun 2013 dengan analisis kesalahan 6,5%.

<hr>This Thesis discuss about the study of a group report data on Indonesian Internet traffic anomalies carried by ID-SIRTII Corporation as a national Agency‟s CSIRT (Computer Science Incident Response Team) of Indonesia. Analyze the way to determine the varians of malware and each signature, behavior, and the impact by using the method of dynamic analysis with web-based tools media support. Implementing forecasting analysis method with time series algorithm to determine the trend of Indonesian malware as well as prediction. Indonesian internet traffic had 21 biggest categories of anomaly with 39.121.466 total incidents during 2012, while 54% made up of different types of SQL attacks and 15% is of botnet attacks. Network incident by Worm is the anomaly predicted to grow continuously in 2013 with 6,5% of error analysis percentage.