Abstract

We present a worm warning system that leverages the reliability of IP-Flow and the effectiveness of machine learning techniques. Our system aims at setting an alarm in case a
node is behaving maliciously. Typically, a host infected by a scanning or an email worm initiates a significant amount of traffic that does not rely on DNS to translate names into numeric IP addresses. Based on this fact, we capture and classify NetFlow records to extract features that uniquely identify worm's flow. The features are encapsulated into a set of feature patterns to train the support vector machines (SVM). A feature pattern includes: no of DNS requests, no of DNS responses, no of DNS normals, and no of DNS anomalies, for each PC on the network within a certain period of time. The SVM training is performed by using five of the most dangerous scanning worms: CodeRed, Slammer, Sasser, Witty, and Doomjuice as well as five email worms: Sobig, NetSky, MyDoom, Storm and Conficker. Eleven worms have been used during the test: Welchia, Dabber, BlueCode, Mytip, Nimda, Sober, Bagle, Francette, Sasser, MyDoom, and Conficker. The results of experiments manifest the soundness of the worm warning system.

References

- W. Wang and D.-S. Luo, “A New Attempt to Detect Polymorphic Worms Based on Semantic Signature and Data-Mining,” in First International Conference of IEEE Communications and Networking (ChinaCom ’06), Beijing, China, October 2006, pp. 1–3.
- Y. Musashi and K. Rannenberg. "Detection of mass mailing worm-infected pc terminals by observing dns query access," IPSJ SIG Notes, pages 39-44, 2004
Index Terms

Computer Science

Security

Keywords

Intrusion detection systems

NetFlow

Support vector machines

Scanning worms

Email worms