Abstract

In recent years, the security threats imposed by email-based malware, modeling the propagation analysis and prevention of email malware becomes a fundamental technique for predicting its potential damages and developing effective countermeasures. Compared to earlier versions of mail malware, modern email malware exhibits two new features. One is reinfection and another one is self-start. In reinfection, whenever any healthy or infected recipients open the malicious attached file the modern email malware sends its copy to the recipients contact. In self-start, whenever compromised computers restart or malicious files are visited the malware spreads over the system. To avoid these types of issues the security specialists use some of the possible techniques and methods to stop and remove the threats. At the same time the malware developers exploit new malware that bypass implemented security features. In this paper, we analyzed the malware propagation and detecting mechanisms. This survey paper highlights the existing detection and analysis methodologies used for these malicious code.
References

Index Terms

Computer Science

Networks

Keywords

Email malware, SIS Model, SIR Model, SII model, ACT, SEIR Model.