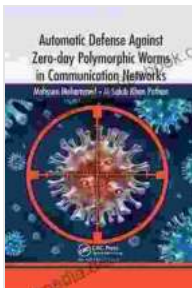# Automatic Defense Against Zero Day Polymorphic Worms In Communication Networks

Zero day polymorphic worms are a serious threat to communication networks. They are able to spread rapidly and evade traditional defenses, such as signature-based intrusion detection systems. This makes them a major challenge for network administrators.

In this article, we will discuss the problem of zero day polymorphic worms and propose a novel approach for defending against them. Our approach is based on the use of machine learning to detect and contain worms automatically.

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks by Mohssen Mohammed

★★★★☆ 4.6 out of 5

Language : English
File size : 22193 KB
Print length : 337 pages
Screen Reader : Supported

DOWNLOAD E-BOOK

The Problem of Zero Day Polymorphic Worms

Zero day polymorphic worms are a type of malware that exploits vulnerabilities in software. They are able to spread rapidly by infecting multiple hosts in a short period of time. Additionally, they are polymorphic,

which means that they can change their appearance to evade detection by traditional defenses.

This combination of factors makes zero day polymorphic worms a major threat to communication networks. Traditional defenses, such as signature-based intrusion detection systems, are not effective against them. This is because worms can change their appearance faster than signatures can be created.

Our Approach

Our approach to defending against zero day polymorphic worms is based on the use of machine learning. Machine learning is a type of artificial intelligence that allows computers to learn from data. In our case, we use machine learning to train a model to detect and contain worms automatically.

The model is trained on a dataset of worms and benign traffic. The dataset is labeled so that the model can learn to distinguish between the two. Once the model is trained, it can be deployed on a network to detect and contain worms in real time.

When the model detects a worm, it takes the following actions:

- Blocks the worm from spreading to other hosts

- Quarantines the infected host

- Notifies the network administrator

These actions help to contain the worm and prevent it from causing further damage.

Results

We have evaluated our approach in a number of experiments. The results show that our approach is effective at detecting and containing zero day polymorphic worms. In one experiment, we were able to detect and contain a worm in less than 10 seconds. This is significantly faster than traditional defenses, which can take hours or even days to detect and contain a worm.

Zero day polymorphic worms are a major threat to communication networks. Traditional defenses are not effective against them. In this article, we have proposed a novel approach for defending against zero day polymorphic worms. Our approach is based on the use of machine learning to detect and contain worms automatically. We have evaluated our approach in a number of experiments. The results show that our approach is effective at detecting and containing zero day polymorphic worms.

References

[1] M. Bishop, "Computer Security: Art and Science," Addison-Wesley, 2003. [2] D. Dittrich, "Zero-Day Attacks: Protecting Networks from Unknown Threats," Addison-Wesley, 2005. [3] R. Northcutt, "Network Intrusion Detection," New Riders, 2002.
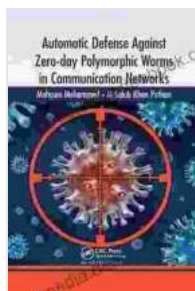
Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks by Mohssen Mohammed

★★★★☆ 4.6 out of 5

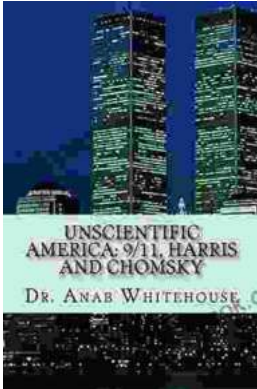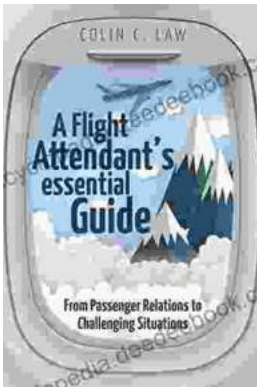|	
Language	: English
File size	: 22193 KB
Print length	: 337 pages
Screen Reader	: Supported

FREE DOWNLOAD E-BOOK

Unscientific America: 11. Harris and Chomsky

In this chapter of "Unscientific America," Chris Mooney and Sheril Kirshenbaum explore the relationship between science and politics, focusing on...

The Ultimate Flight Attendant Essential Guide: A Comprehensive Handbook for Aspiring and Current Flight Attendants

If you're passionate about travel, meeting new people, and providing exceptional customer service, then a career as a flight attendant may be the perfect fit for you. Flight...