Topics in Network Security
Project Report

Suspicious Mail Detection

Noa Tshuva **315856609**
Nitzan Hochman **316264845**

Supervisor: Doron Ofek

אוניברסיטת בן-גוריון בנגב
Ben-Gurion University
of the Negev

Department of Computer Science
Ben-Gurion University of the Negev

Abstract

This project was part of the Topics in Network Security course, which required us to read the materials and build a project that implements an antivirus program of our choice. We have decided that our antivirus will consist of a suspicious mail detector, since we both have found the different types of threats that can be sent over email interesting and also the way of protecting the client against them.

The Implementation

Our project consists of a mail server and 5 clients which are mail senders. Each client sends different messages with different attachments or links, 4 of them are malicious/suspicious and one is clean.

The server has several different methods for checking if the mail is suspicious:

It checks if the attachments have virus signatures in them.

A virus signature is a continuous sequence of bytes that is common for a certain malware sample. That means it's contained within the malware or the infected file and not in unaffected files. virus signatures are not really used today to detect viruses.

We use a signatures file which contains different virus signatures. Our server goes through the file and saves all of the viruses in a virus struct list, which it then uses to identify 'infected' files, which are files that contain a virus signature.

It checks if the link attached is a redirected link

When launching a mass mailing spammers always try to hide their client's contacts – the telephone number, the site, etc.; otherwise, any spam filter can put such contacts on a deny list and block all mass mailings where it is mentioned. In an effort to bypass filtration systems, spammers use a variety of methods – they create background "noise" in messages using extra symbols or image distortion, write numbers in words, add HTML tags invisible to users, place contact information on "noisy" images, etc.

In 2011, the spammers favorite trick for hiding a link to advertising or malicious sites was redirection: the email contained a link to a web page which redirected the user to the main site.

Our server has a function which checks if the link given is a redirected link – and if it is, regards it as spam.

It checks if the file type written is the same as the type of the attached file

We wrote the project in Python and used SMTPd library to create SMTP severs and clients, we used a virus signatures list and an "infected file" from previous course (Architecture).

The most challenging parts were deciding how to implement the mail detector idea, implementing a mail server – since it was a first for both of us, and implementing the virus signature test.

It checks if the name of the file is suspicious

In Conclusion

In spite of the hardships, we are content with the result and the experience. We learned a lot about suspicious mail detection, and about different ways hackers use mail as a way to manipulate people into surrendering their data/resources /personal information. We learned about mail servers and SMTP in particular.