

Avira SPACE

- Spam and Phishing Protection -

A security option for iQ.Suite Wall



Contents

- 1 Introduction2
- 2 Avira SPACE Methods and Techniques in Detail2
 - 2.1 Spam Detection.....2
 - 2.1.1 Advanced Text Analysis.....2
 - 2.1.2 Known Words Analysis2
 - 2.1.3 Bayesian Filtering2
 - 2.1.4 Real-time Blacklists3
 - 2.2 Phishing Detection3
 - 2.2.1 Static Methods.....3
 - 2.2.2 Dynamic Methods.....3
- 3 About Avira4
- 4 About GROUP Business Software5

1 Introduction

Avira SPACE (Spam and Phishing Advanced Cross platform Engine) is an option for the anti-spam solution iQ.Suite Wall to detect spam and phishing emails. The solution can be used under Lotus Notes Domino as well as Microsoft Exchange.

Avira SPACE makes use of different methods and technologies to achieve the highest possible protection against spam and phishing emails:

- Advanced Text Analysis (ATA) searches for constructions very often used in spam or phishing emails
- Known Word Analysis searches emails for obfuscated words
- Bayesian filtering uses statistical methods based on words that have been seen by the system in spam or ham mails
- In addition to the overall protection scheme the solution looks online for well-known spam sender domains on real-time blacklisting servers
- A special phishing detection engine uses a combination of static and dynamic methods to detect phishing emails in particular.

2 Avira SPACE Methods and Techniques in Detail

2.1 Spam Detection

2.1.1 Advanced Text Analysis

The Advanced Text Analysis (ATA) searches the received message for common anomalies, usually present in spam mails in an attempt to trick mail filters or to disguise the origin of the email etc. It also contains some extensive tests to detect possible phishing emails.

2.1.2 Known Words Analysis

The text from the email is searched for various obfuscated words (space or punctuation insertion between letters, for example), with the help of regular expressions. If the mail contains both text/html and text/plain, SPACE detects if they are similar or not (they should be similar).

2.1.3 Bayesian Filtering

The Bayesian filter uses a combination of statistical methods to detect possible spam emails based on the previous knowledge that the words were seen in spam or ham emails. The solution is able - out of the box - to detect spam, phishing and sometimes malware which spread via email.

If the other methods detect an email as a sure SPAM or sure HAM, the product will train itself (using the Bayesian module) with that email as SPAM or HAM respectively. As a result the de-

tection will become better and better over time with the help of the Bayesian module without the user having to interfere.

2.1.4 Real-time Blacklists

Each email contains an IP address of the mail server it was sent from. Avira SPACE takes these IP addresses and queries a number of blacklist servers in the internet if those domains are listed as well-known spam IP addresses and gives some spam points for them.

2.2 Phishing Detection

2.2.1 Static Methods

These methods represent a combination of tests to decide if an email is phishing or not. The trigger for this detection is a “known” domain or name in the From: header of the mail. To give an example: If SPACE encounters an email coming from “security@paypal.com”, the solution switches into “possible phishing mode” and will mark the mail as phishing depending on different conditions, e.g. it contains a spoofed link; it is a link to a domain different from paypal.com; it contains suspicious text (like “Click here to activate your account”) and various other constructions.

2.2.2 Dynamic Methods

The following two methods use the same data in order to take a decision, but two different algorithms. Avira SPACE analyses the email and extracts certain pieces of information from it to create a characteristic profile of the message. Currently, more than 40 elements are considered. This information is used to decide whether an email is trustworthy or not, i.e. if it is phishing or not. What happens in the background is that the underlying detection algorithm takes the information about those characteristic elements and learns how to combine them in new and different ways to detect new spam emails.

Decision Tree

The decision tree (a method from the machine learning discipline) is able to classify the feature vectors into 4 different categories: normal, real-mail, possible phishing and phishing.

Phishing Points

This method uses a scoring method and works by adding “phishing points” to a total score, depending on the flags from the feature vector. When the sum of phishing points exceeds a threshold, the mail is marked as phishing.

3 About Avira

Avira is a leading global provider of IT security solutions for professional and private use. With over twenty years of experience, the company is one of the pioneers in this field. As a foundation member of the initiative “IT Security made in Germany” (ITSMIG e.V.), Avira guarantees that it provides IT security products with no backdoors.

The German IT security expert is headquartered in Tettnang near Lake Constance and maintains several subsidiaries worldwide. Avira employs approximately 300 staff and makes a significant contribution towards the security of millions of private users through its free virus protection, Avira AntiVir Personal.

Domestic and international customers include well-known companies listed on global stock exchanges, educational establishments and government authorities. In addition to protecting the virtual environment, Avira promotes the Auerbach Foundation for greater protection and security in the real world. The Auerbach Foundation supports charitable and social projects, as well as art, culture and science.

4 About GROUP Business Software

GROUP Business Software is the leading provider of IBM Lotus based solutions and services in the fields of Email Management and Archiving, Cloud Computing, CRM, Corporate Compliance and Administration. The GROUP business units offer "Collaborative Business Solutions" to support companies and end users in their daily work and to simplify business processes.

While competitors only offer partial solutions for collaborative systems, GROUP provides a comprehensive and harmonized solution portfolio which includes all areas of collaboration. By integrating GROUP solutions in business processes, companies and organizations achieve their goals easier, faster and more efficiently.

Competencies

Central: GROUP solutions make it possible to manage and control business-critical process from a central location, thus relieving both administrative staff and end users in their daily work. With all users included on a company-wide basis using a server-based system, all of their operations can be controlled and managed from a central interface.

Uncomplicated: GROUP solutions feature outstanding usability and unmatched efficiency. While reducing the necessary user interaction to a bare minimum, the server-based solutions provide intelligent automatisms that contribute to increasing productivity and cost-effectiveness.

Compliant: Centrally defined processes ensure compliance with corporate policies and statutory requirements. Intuitive configuration options allow to flexibly adapt the solutions used to specific market requirements, corporate specifications or new laws.

Customers

GROUP is based in Europe and the USA. Companies worldwide rely on GROUP solutions for the security, organization and efficiency of their systems. GROUP customers include well-known companies from all over the world, such as Deutsche Bank, Ernst & Young, Honda, Heineken, Allianz and Miele.

For further information please visit www.gbs.com

© 2010 GROUP Business Software AG

Our product descriptions are of a general and descriptive nature only. They do not stipulate any specific features nor do they represent any form of warranty or guarantee. We reserve the right to change the specifications and design of our products without notice at any time, in particular in order to keep abreast of technical developments. The information contained in this document presents the topics from the viewpoint of GROUP Business Software AG at the time of publishing. Since GROUP Business Software AG needs to be able to react to changing market requirements, this is not an obligation for GROUP Business Software AG and GROUP cannot guarantee that the information presented in it is accurate after the publication date. This document is intended for information purposes only. GROUP Business Software AG does not extend warranty for this document, in either explicit or implied form. This also applies to quality, execution, standard commercial practice or suitability for a particular purpose. All the product and company names that appear in this document may be trademarks of their respective owners.

European Headquarters

GROUP Business Software AG

MesseTurm
60308 Frankfurt / Germany
Phone: +49 69 789 8819-0
Fax: +49 69 789 8819-99

North American Headquarters

GROUP Business Software Corporation

40 Wall Street, 33rd Floor
New York, NY 10005 / USA
Phone: +1 212 995-2900
Fax: +1 212 995-2206

Email Main Office

GROUP Business Software AG

Ottostrasse 4
76227 Karlsruhe / Germany
Phone: +49 721 4901-0
Fax: +49 721 4901-199

UK Office

GROUP Business Software (UK) Ltd.

3 More London Riverside
London SE1 2RE / UK
Phone: +44 207 206 0001

info@gbs.com
www.gbs.com

 GROUP