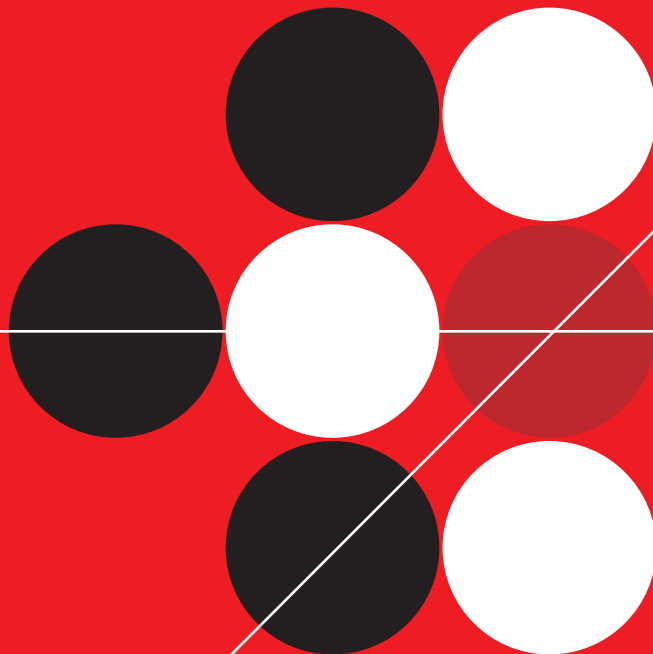


# TREND MICRO™

## Email Reputation Services 3

Dynamic Spam Protection at the Network Layer

Getting Started Guide





Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before using the service, please review this Getting Started Guide.

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Trend Micro, the Trend Micro t-ball logo, InterScan, TrendLabs, Trend Micro Control Manager, and Trend Micro Damage Cleanup Services are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 1995-2007 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. <<update IBEM 22591/51216>>

Release Date: April 2007

Protected by U.S. Patent No. 5,623,600; 5,951,698; 5,983,348; 6,272,641

The Getting Started Guide for Trend Micro Email Reputation Services is intended to provide in-depth information about the main features of the service. You should read through it prior to using the application.

For technical support, please refer to the Contact Information and Web-based Resources appendix for information and contact details. Detailed information about how to use specific features within the appliance are available in the online help file and online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please email us at the following address:

`docs@trendmicro.com`

Your feedback is always welcome. You can evaluate this documentation at the following Web site:

<http://www.trendmicro.com/download/documentation/rating.asp>

# Contents

## Preface

Email Reputation Services Documentation .....	iv
Audience .....	iv
Document Conventions .....	v

## Chapter 1: Introducing ERS

About Email Reputation Services (ERS) .....	1-2
Trend Micro Email Reputation Services Standard .....	1-2
Trend Micro Email Reputation Services Advanced .....	1-3
Trend Micro Threat Prevention Network .....	1-3
Mail Abuse Prevention System (MAPS) .....	1-4
Reputation Assignment .....	1-4
Delivery Infrastructure .....	1-5
How ERS Works .....	1-6
Blocking Connections vs. Messages .....	1-7
Spam Count without Blocking .....	1-7

## Chapter 2: Getting Started with ERS

Configuring Email Reputation Services .....	2-2
Signing up for Service and Obtaining Service Activation Code ...	2-2
Configuring Your MTA .....	2-3
Testing Your Server .....	2-4
Reporting .....	2-4
Creating an Account for the ERS Console .....	2-5
Software Required for Accessing the Administration Console ..	2-5
Creating an Account .....	2-5

## Chapter 3: Using the Administration Console

Logging on to the Administration Console .....	3-2
Getting Help with the Administration Console .....	3-2
Global Spam Update .....	3-4
Reports .....	3-5
Percent Listed Report .....	3-5

Hourly and Daily Reports .....	3-6
Botnet Reports .....	3-7
Policy .....	3-8
ISP Tools — ISP Report .....	3-9
ASN Report .....	3-9
IP Report .....	3-9
Administration .....	3-11
Changing the System Password .....	3-11
Valid Mail Server Administration .....	3-12

## **Appendix A: Contact Information and Web-based Resources**

Contacting Technical Support .....	A-2
General Contact Information .....	A-3
Supported Performance Levels .....	A-3
Service Availability .....	A-3
Email Delivery .....	A-3
Knowledge Base .....	A-4
Sending Suspicious Code to Trend Micro .....	A-5
TrendLabs .....	A-6
Security Information Center .....	A-7

# Preface

Welcome to the *Trend Micro™ Email Reputation Services 3.0 Getting Started Guide*. The guide introduces the main features of the service and installation instructions for your production environment. Please read through this guide prior to installing or using the service.

This preface discusses the following topics:

- *Email Reputation Services Documentation* on page iv
- *Audience* on page iv
- *Document Conventions* on page v

## Email Reputation Services Documentation

The Email Reputation Services (ERS) documentation consists of the following:

**Online Help**—Online help—Helps you configure all features through the user interface. You can access the online help by opening the Web console and then clicking the help icon (🔗).

**Getting Started Guide**—Helps you plan for deployment and configure all service settings.

## Audience

The ERS documentation is written for IT managers and email administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of email messaging networks, including details related to the following:

- SMTP protocol
- Message transfer agents (MTAs)

---

**Note:** Knowledge about configuring an MTA to make DNS RBL query is essential.

---

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

## Document Conventions

To help you locate and interpret information easily, the ERS documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
Monospace	Examples, sample command lines, program code, Web URL, file name, and program output
<u>Note:</u>	Configuration notes
<u>Tip:</u>	Recommendations
<u>WARNING!</u>	Reminders on actions or configurations that should be avoided



# Introducing ERS

Trend Micro™ Email Reputation Services (ERS) delivers high-performance, cost-effective hosted security services, protecting businesses against spam, viruses, and inappropriate content before they reach your network.

Topics in this chapter:

- *About Email Reputation Services (ERS)* on page 1-2
- *Trend Micro Email Reputation Services Standard* on page 1-2
- *Trend Micro Email Reputation Services Advanced* on page 1-3
- *Trend Micro Threat Prevention Network* on page 1-3
- *How ERS Works* on page 1-6

## About Email Reputation Services (ERS)

As the first line of defense, Trend Micro™ Email Reputation Services (ERS) stops more than 80% of spam at its source — before it can flood your network, overload mail gateway security, and burden system resources. To block spam, the IP address of incoming mail is verified against the world's largest, most trusted reputation database-managed by Trend Micro Threat Prevention Network. Real-time spam blocking identifies new sources of spam, even zombies and botnets, as soon as they begin spamming.

When your mail server encounters an incoming message with an IP address from an unknown host, it makes a DNS query to the Trend Micro reputation databases. If the host is listed in the database, ERS recommends an appropriate action, depending on the database in which it appears. The ERS family includes Trend Micro Email Reputation Services Standard and Trend Micro Email Reputation Services Advanced. Email Reputation Services Standard is powered by the most comprehensive reputation database and includes ratings for over 1.6 billion IP addresses with history and spamming activity. Email Reputation Services Advanced combines the services of Standard Reputation database with dynamic real-time anti-spam technology that can identify suspect behavior and immediately block new sources of spam.

Over the past year many customers have seen their spam volume grow more than 90%, and spammers continue to evolve new techniques including the use of botnets and zombies.

## Trend Micro Email Reputation Services Standard

Trend Micro Email Reputation Services Standard blocks spam at its source by validating IP addresses against the industry's most comprehensive and reliable standard reputation database, powered by Trend Micro Threat Prevention Network. This ever-expanding database currently contains 1.6 billion IP addresses with reputation ratings based on spamming activity. Trend Micro's spam investigators continuously review and update these ratings to ensure accuracy.

This service was originally created in 1996 by team of investigators under the name Mail Abuse Prevention System (MAPS). MAPS is now a part of the Trend Micro Threat Prevention Network. Over the years this professional organization has developed detailed methodologies for identifying and managing sources of spam and

network security threats. The result is the most accurate and comprehensive repository of network intelligence in the industry.

Email Reputation Services Standard is a DNS query-based service. Your designated mail server makes a DNS query to the standard reputation database server whenever an incoming mail message is received from an unknown host. If the host is listed in the standard reputation database, you choose the appropriate action to be taken with that mail. We recommend that you block, and not receive, any mail from an IP address that is included on the standard reputation database.

## Trend Micro Email Reputation Services Advanced

Trend Micro Email Reputation Services Advanced is a dynamic real-time solution that identifies and stops sources of spam while they are in the process of sending millions of messages. To achieve this, our team of spam experts continuously monitors network and traffic patterns and immediately updates the reputation database as new spam sources emerge, often within minutes of the first sign of trouble. As evidence of spam activity ceases, the reputation database is updated accordingly.

Email Reputation Services Advanced is a DNS query-based service like Email Reputation Services Standard. At the core of this service is the standard reputation database, along with the dynamic reputation database, a dynamic real-time database. These two databases have distinct entries and there is no overlap of the IP addresses, allowing us to maintain a highly efficient and effective database that can quickly respond to zombies, BGP attacks and other highly dynamic sources of spam.

Email Reputation Services Advanced has blocked more than 80% of total incoming connections in customer networks. Results will vary depending on how much of your incoming mail stream is spam. The more spam you receive, the higher the percentage of blocked connections you will see.

## Trend Micro Threat Prevention Network

ERS is powered by the Trend Micro Threat Prevention Network, a global network operated by highly-trained spam investigators who research, collect, process, and distribute reputation ratings on IP addresses. These specialists monitor spam activity, develop information on spam sources, verify the accuracy of reputation ratings, and work with organizations to ensure the service is tracking spammers correctly.

Working around the clock to assure 100% availability and millisecond response times, the Threat Prevention Network delivers real-time updates to the database for immediate availability. This high level of service is the key component for building and maintaining the world's most reliable, reputation database-unmatched in the industry. For more information about Threat Prevention Network service and support, go to: [www.trendmicro.com/services/tpn/](http://www.trendmicro.com/services/tpn/).

## Mail Abuse Prevention System (MAPS)

As part of the Threat Prevention Network, the MAPS Threat Analysis team (formerly Mail Abuse Prevention System) maintains the reputation databases to ensure ratings are accurate and up-to-date. Every rating includes comprehensive spamming histories and spam samples for complete transparency into the databases. This service is unique because it is fully auditable by anyone who has questions regarding an assigned rating.

### Reputation Assignment

The investigators on the Threat Analysis team follow stringent policies and guidelines for the nomination and removal of IP addresses from the databases that are part of the Email Reputation Services Standard. Each IP address has a reputation that has been assigned based on meeting at least one of the following criteria:

- The IP address has sent spam or in some way has supported the sending of spam (i.e. offering services to spammers or allowing their resources to be used by those who send spam).
- The IP address is an unsecured mail server ("open relay") that has been used to send spam
- The IP address is an unsecured port on a machine ("open proxy") that has been used to send spam
- The IP address is a dynamically assigned address that should not be used as a mail server

Each IP address that is nominated is categorized before it is processed according to careful guidelines to assure that the reputation assigned is appropriate and correct. The same investigator that assigned the reputation can also mediate any requests to change the assigned reputation. Every effort is made to assure the accuracy of the reputation and ensure changes are made in a timely manner.

Each reputation for an IP will include samples of the actual spam sent, history of spamming behavior, record of any correspondence regarding mediation, resolution of issues, and other related information. For dynamically assigned IP addresses that were submitted to the standard reputation database by the ISP, their records will include submission dates and any limitations placed upon that IP by the ISP.

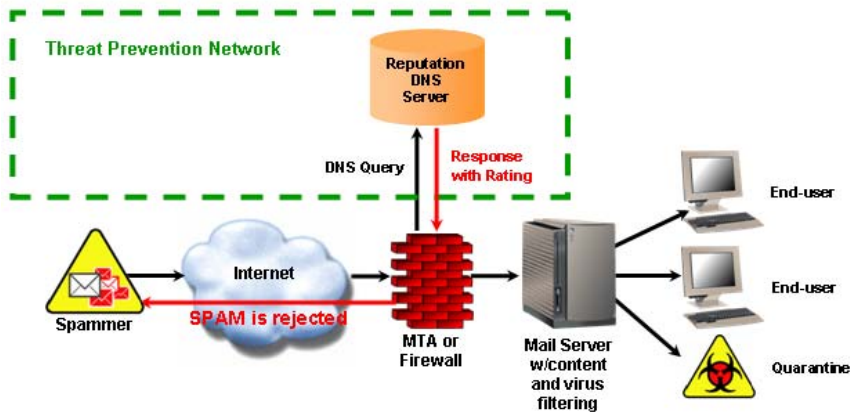
The reputation of an IP address can be viewed by using the IP Lookup Tool found on the MAPS website: [www.mail-abuse.com/cgi-bin/lookup](http://www.mail-abuse.com/cgi-bin/lookup).

## **Delivery Infrastructure**

Trend Micro has built some of the largest IP networks and data centers in the world. Our network DNS and database servers are geographically distributed in major co-location facilities, and we continuously monitor and tune our network to assure 100% availability. The network currently consists of eight data centers distributed throughout the world located in Atlanta, GA; Los Angeles, CA; Reston, VA; San Francisco, CA; San Jose, CA; Seattle, WA; Munich, Germany; and Tokyo, Japan. We will deploy additional locations in anticipation of regional demand. Our network is continually being optimized and expanded to maintain the highest availability possible for our customers.

## How ERS Works

The actual implementation of ERS involves up to two DNS look-ups per IP address. When a mail server accepts the initial connection from another mail server, it records the IP address of the machine requesting the connection. The receiving mail server will query its DNS server, which in turn queries the Reputation DNS server to determine if there is a record for that IP address.



**FIGURE 1-1 Threat Prevention Network Workflow**

For Email Reputation Services Standard, there is a single DNS query made to the standard reputation database which contains known and documented sources of spam, as well as an extensive listing of dynamic IP addresses. Any positive response from this database should result in your mail server returning a '550' error, or rejection of the requested connection.

For Email Reputation Services Advanced, if the first query to the standard reputation database does not return a positive response then a second query is made to the dynamic reputation database, a dynamic threat database. A positive response from this database should result in your mail server returning a '450' error, or 'temporary failure' of the requested connection. Listings in this database are occasionally legitimate mail servers that have compromised hosts behind them that are temporarily sending spam. If the connection request is from a legitimate mail server

it will re-queue and try again later, causing a delay in mail delivery until the listing expires but not blocking mail.

Depending on your mail server's capabilities, additional options for handling IP connections may be available to you. Some allow for throttling or limiting the number of connections accepted from an IP over a designated time period. Still others allow you to set different levels of scanning to messages from questionable IP addresses as opposed to known IP addresses. The ultimate goal is to reject as many connections upon initial request as possible; therefore spam messages are never accepted and never brought into the mail infrastructure. Keeping unwanted spam out of the infrastructure means that valuable bandwidth, processing and storage resources are not wasted.

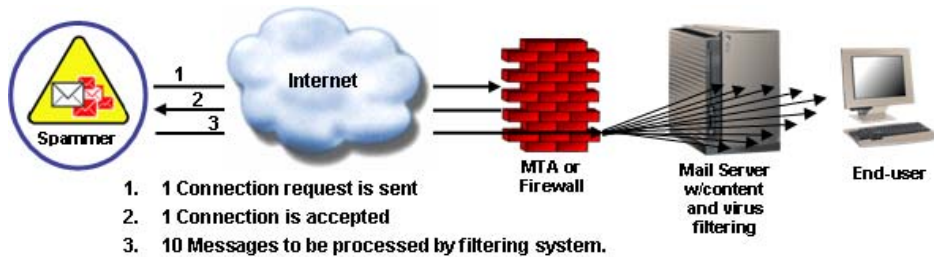
## Blocking Connections vs. Messages

Our customers find that adding ERS to their anti-spam solutions has an exponential impact on offloading existing filtering solutions. What can appear to be only a small increase in blocked connections can translate into a large reduction of actual messages entering the filtering portion of their mail infrastructure.

Translating blocked connections into blocked messages is more involved than simply applying a 1:1 ratio. Studies show that while legitimate sources average slightly over one message per connection, each connection from a spam source contains conservatively an average of ten messages.

## Spam Count without Blocking

An example of how this works: an organization is getting 1,000,000 connection requests a day. If each blocked connection is being counted as equivalent to each message filtered and 40% of all messages are being blocked and an additional 40% are being filtered, it would appear that the blocking functionality is equally effective as the filtering functionality of the anti-spam solution.



**FIGURE 1-2 Spam Count without Blocking Message Flow**

If you apply the 10:1 multiplier to the connection portion of the solution, suddenly what looked like 400,000 messages out of 1,000,000 messages were being stopped (600,000 were being passed to the filtering application) now become 4,000,000 messages out of 4,600,000 messages, or 87% of total messages are being stopped by the blocking portion of the solution and only 9% is being filtered. Now the blocking function takes on a much more significant role in protecting the infrastructure.

If you take it down a level to the infrastructure required to process these connections and messages, it is far more efficient to reject at the connection level rather than take each message through full content scanning. Blocking at the IP level involves the initial portion of the SMTP handshake to determine the connecting IP address and then a simple DNS query. Whereas to fully scan each message requires the full SMTP handshake take place for each connection and then complete message parsing for each message contained within that connection (average 10:1 for spam). In addition, repeat offending IP addresses within a short period of time (e.g., spam flood) can be caught using a local cache for even higher efficiency.

# Getting Started with ERS

This chapter discusses the following topics:

- *Configuring Email Reputation Services* on page 2-2
- *Signing up for Service and Obtaining Service Activation Code* on page 2-2
- *Configuring Your MTA* on page 2-3
- *Creating an Account for the ERS Console* on page 2-5

## Configuring Email Reputation Services

It is a simple process to enable and configure Email Reputation Services (ERS). You should see immediate results upon implementing this service. The level of spam entering your network and requiring further processing will drop dramatically.

The most effective way to deploy Email Reputation Services is for it to be the first line of defense in your messaging infrastructure. Most mail systems have a multilayer structure that often includes some pre-existing DNS blocking, spam filtering, and virus filtering. Trend Micro recommends that other DNS blocking techniques be removed completely from the messaging environment and ERS act as the precursor to any application filtering you may utilize.

The ERS configuration process includes four steps:

- Step 1 — *Signing up for Service and Obtaining Service Activation Code* on page 2-2
- Step 2 — *Configuring Your MTA* on page 2-3
- Step 3 — *Creating an Account for the ERS Console* on page 2-5

## Signing up for Service and Obtaining Service Activation Code

Whether you sign up for the trial evaluation or are purchasing the service, you first need to submit some basic information for account management and provisioning of the service.

If you are signing up for a trial, you need to complete the request form appropriate for the service level you wish to evaluate.

### **Email Reputation Services Standard:**

<https://nssg.trendmicro.com/download/trial/trial-services.php?id=66>

### **Email Reputation Services Advanced:**

<https://nssg.trendmicro.com/download/trial/trial-services.php?id=65>

If you register for the trial, an Activation Code will be provided via email along with instructions for configuring your MTA. This Activation Code will only be good for the length of the evaluation and you will need to obtain a new Activation Code when you purchase the service.

If you purchase the service, you will receive a Registration Key that will allow you to create a customer account with Trend Micro and upon completion of the registration process you will receive your Activation Code.

The Activation Code will only allow you access to the level of service to which you are registered; Email Reputation Services Standard or Email Reputation Services Advanced. Please note that the Activation Code for Email Reputation Services Advanced includes access to Email Reputation Services Standard which is a sub-component.

---

**Note:** It may take up to one hour from when your Activation Code is issued before it is recognized by the Email Reputation Services systems.

---

## Configuring Your MTA

The next step is to configure your MTA to perform the appropriate DNS queries for the subscribed Email Reputation Service.

- **For Trend Micro Email Reputation Services Standard:** When configuring your MTA, you need to set it up to reject connections with a 550 level error code (connection refused), which indicates that a positive response was received from the standard reputation database. Listings in the standard reputation database are known to be spammers or sources that should not be sending email, so rejecting these connections outright is the standard method for handling them.
- **For Trend Micro Email Reputation Services Advanced:** You will need to configure your MTA to potentially make two DNS queries. If a positive response is not received from the first query to the standard reputation database, then your MTA will need to make a second query to the dynamic reputation database. Your MTA should temporarily deny connections with a 450 level error code (server temporarily unavailable, please retry), when a positive response is received from this database.

Listings in this database are occasionally legitimate mail servers that may have compromised hosts behind them that are temporarily sending spam. If the connection request is from a legitimate mail server it will re-queue and try sending the message at a later time. This will cause a short delay in mail delivery until the listing expires, but will not permanently block the mail.

Some servers may have additional options for handling questionable IP connections such as throttling or routing messages for more detailed scanning. Some customers have chosen to utilize these capabilities for managing IP addresses on the dynamic threat database.

Instructions for configuring your MTA, or firewall, can be found on the Trend Micro website.

**Email Reputation Services Standard:**

<http://www.trendmicro.com/en/products/nrs/rbl/use/configure.htm>

**Email Reputation Services Advanced:**

<http://www.trendmicro.com/en/products/nrs/nas/use/configure.htm>

The instructions have been provided by the vendor or manufacturer of the product. We will assist you in the configuration process, but you may wish to refer to your product's manuals and/or technical support organization for detailed configuration and set-up options.

---

**Note:** Insert your unique valid Activation Code to replace the instructional text example; do not include any dashes.

---

## Testing Your Server

Once you have configured your server, you may send an email to [ers\\_support@trendmicro.com](mailto:ers_support@trendmicro.com) to request that a test email be sent to you. It will test whether your mail server is configured to use the services properly.

## Reporting

Before and after deployment of Trend Micro ERS, you may want to track the effectiveness of your anti-spam solution, both at the network and application levels. Most MTA products provide some level of reporting that can be customized to meet your needs. Because the capabilities of these products vary from vendor to vendor, be sure to reference the documentation for your particular SMTP gateway, or contact the vendor for assistance in developing and understanding the reports available to you.

## Creating an Account for the ERS Console

You can access global spam information, view reports, create or alter policies for Approved Sender IP and Blocked Sender IP lists, and perform administrative tasks by logging on to the ERS administration console.

### Software Required for Accessing the Administration Console

To create and access your ERS administration console, one of the following browsers is required.

- Microsoft™ Internet Explorer 6.0
- Mozilla™ Firefox™ 1.5.0

### Creating an Account

To create an account:

1. Point your browser to the URL for the administration console to access the logon page.



FIGURE 2-1 ERS Login Screen

2. Click **Register a New Account**.

**New Account Request**

Please enter your **Username**, **Email** address and **Activation Code**. If the **Activation Code** entered is successfully authenticated, a temporary password will be sent to your email address. Otherwise, no password will be sent and no account generated. If you forgot your Activation Code, please contact [Trend Micro ERS Support](#).

**Note:** you may use an activation code only once!

Username:

Email:

Activation Code:

**FIGURE 2-2 ERS New Account Request Screen**

3. Complete the **New Account Request** form. You will be asked to provide:

- **Username**
- **Email**
- **Activation Code**

---

**Note:** The Activation Code should be the same Activation Code used when configuring your MTA to access ERS.

---

4. Click **Submit**. An email will be sent to you confirming your account has been created, along with a temporary password.

## Using the Administration Console

Once you have created an account for the Email Reputation Services (ERS) administration console you will receive an email confirming your account along with a temporary password. You can now log into the console and begin configuring your Approved and Blocked Senders IP lists.

This chapter covers the following ERS functions:

- *Logging on to the Administration Console* on page 3-2
- *Global Spam Update* on page 3-4
- *Reports* on page 3-5
- *Policy* on page 3-8
- *Administration* on page 3-11

## Logging on to the Administration Console

You can access global spam information, view reports, create or manage Approved Sender IP and Blocked Sender IP lists, and perform administrative tasks by logging on to the ERS administration console.

### To log on to the console:

1. Point your browser to the URL for the administration console to access the logon page.

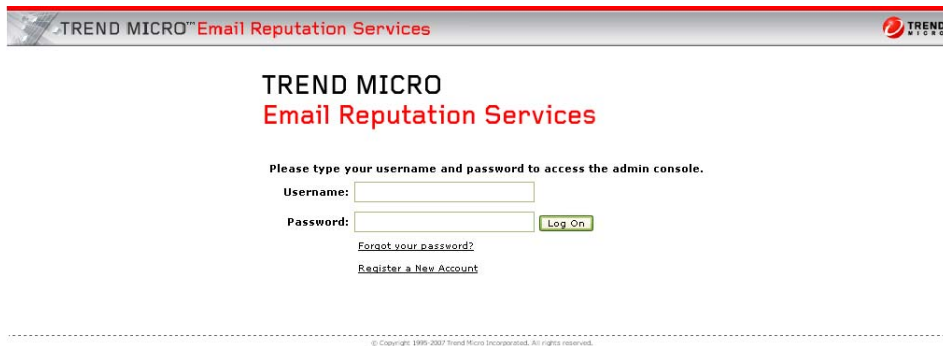


FIGURE 3-1 ERS login screen

2. Type your **Username** and **Password**.
3. Click **Log On**.

**Note:** After you have logged on for the first time, Trend Micro recommends changing your password to help ensure the security of your ERS account. (See the *Administration* on page 3-11.)

## Getting Help with the Administration Console

For detailed information about working with the administration console, see the help files. You can access page-level help for a particular screen by

clicking the blue question mark (  ) near the upper right corner of each screen.



**FIGURE 3-2** ERS online help access icon

## Global Spam Update

When you log on to the console, the Global Spam Update page appears similar to the screenshot below. This page provides a brief overview and discussion of current spamming tactics and their implication for organizations. It describes how new tactics are being deployed and how they have been designed to get through our systems, as well as how we are responding to these new threats.

By selecting the ISP Spam tabs you can see, based on the total Spam Volume received from the top 100 ISPs for a specific week, those networks producing the most spam ranking at the top of the list.

The screenshot shows the Trend Micro Email Reputation Services (ERS) console. The top navigation bar includes 'Log Off', 'Help', and the Trend Micro logo. The left sidebar contains a menu for 'Global Spam Update' with sub-items: Report, Policy, ISP Tools, and Administration. The main content area is titled 'Global Spam Update' and includes a 'Spam Alert' section with tabs for 'ISP Spam.1', 'ISP Spam.2', 'ISP Spam.3', and 'ISP Spam.4'. Below this is a 'Welcome' message from Trend Micro, discussing botnet activity and upcoming features.

**Global Spam Update** Email to Support

**Spam Alert** ISP Spam.1 ISP Spam.2 ISP Spam.3 ISP Spam.4

**Welcome**

Welcome to the latest revision of the Trend Micro's Email Reputation Portal. In this release there is an important new report – Botnet Activity. What is a Botnet? – This is an automated network of computers which have hidden malware code and can be commanded via a remote computer to send Spam or perform other malicious activity. After you have entered your valid Email Server IP addresses Trend Micro will look for Botnet activity for those IP addresses and present this in a 7-day report the next day. You will be able to hover and click on the Botnet icon for a specific sample of the Spam. We highly recommend you send an Email to [Trend Micro Support \(ers\\_support@trendmicro.com\)](mailto:ers_support@trendmicro.com) if you find active Botnets within your network.

Coming soon is an adjustable slider which allows you to set the aggressiveness of the Reputation system on your Email Gateway. You can make the service stop more or less Spam depending on your specific Email environment and policies. Also for our ISP customers we will be including a very detailed reporting tool to track Botnets within their IP space.

Finally we would like to hear what you think of the service and what improvements can be made. We will provide some interactive areas where you can see upcoming new features and make requests of your own.

Sincerely  
Trend Micro

© Copyright 2006, 2007 Trend Micro Incorporated. All rights reserved.

**FIGURE 3-3** ERS Global Spam Update page

## Reports

These reports summarize the query activity between your MTA and the ERS database servers.

If you have registered your valid mail servers' IP addresses using the Administration page, you will also be able to see a daily botnet activity report of your mail servers.

Depending on the service level you have subscribed to, you will either see a blue colored graph if you subscribed to Email Reputation Services Standard, or a blue and yellow colored graph if you subscribed to Email Reputation Services Advanced. If you subscribed to Email Reputation Services Advanced and do not see the yellow portion of the graph, then there is probably something wrong with the configuration of your MTA and you should contact Support for assistance.

### Percent Listed Report

The first graph, Percent Listed, shows the percentage of queries where a positive response was given by the database. A positive response means that there is a reputation rating for the IP address that was queried and that Trend Micro recommended an action against the IP address.

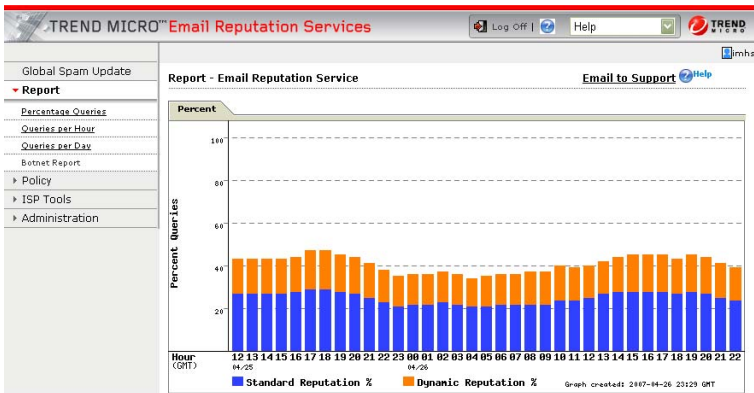


FIGURE 3-4 ERS report — Percent Listed screen

**Note:** This is just a portion of the activity happening at your gateway. Depending on the level of caching set up on your system, this is just a percentage of your total email traffic. Each server has different default settings and each one allows for varying degrees of customization of those settings.

## Hourly and Daily Reports

The next two graphs, Hourly and Daily, show the rate at which your server is querying the ERS database servers, with the rate of queries displayed as number of queries per second. The graph is designed to be read from left to right, with the right showing the most recent query traffic levels.

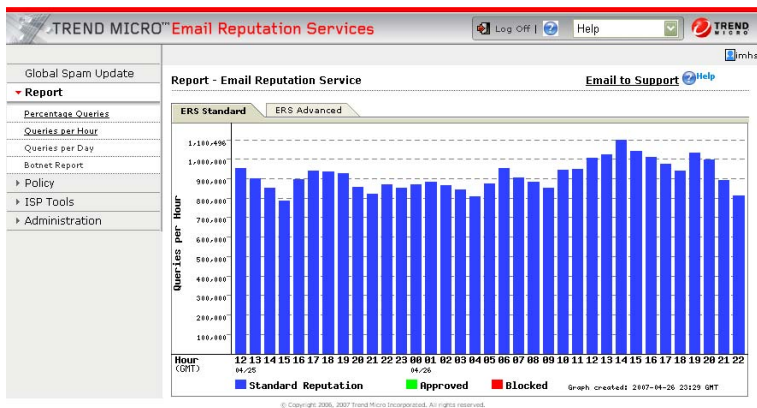


FIGURE 3-5 ERS Daily query report page

## Botnet Reports

The botnet report gives you quick summary of spam activity originating from the servers that you have listed as valid mail servers.

A botnet is a network of computers that have been compromised by spyware, trojans, or other illegitimate software for the purpose of using the compromised computers in order to send out spam email.

If there has been any spam activity on a given day for a specific IP address then a red robot icon is displayed. Click the robot to see a detailed view of the specific spam counts and the date and time of their origin in a popup window.

Within this popup window you will also be able to click a link to view a sample spam message that originated from that server. The sample spam message does have some sections obscured in order to protect the privacy of innocent spam victims.

TREND MICRO™ Email Reputation Services									
Global Spam Update									Log Off   Help
Report									
BOTNET Activity									
Email to Support									
Botnet Activity - Last 7 days									
IP Address	Today	04/25/07	04/24/07	04/23/07	04/22/07	04/21/07	04/20/07		
65.36.255.250	—	—	—	—	—	—	—		
8.10.161.0/24									
12.3.196.1	—	—	—	—	—	—	—		
216.99.131.5	—	—	—	—	—	—	—		
216.99.131.6	—	—	—	—	—	—	—		
216.99.131.7	—	—	—	—	—	—	—		
216.99.131.8	—	—	—	—	—	—	—		

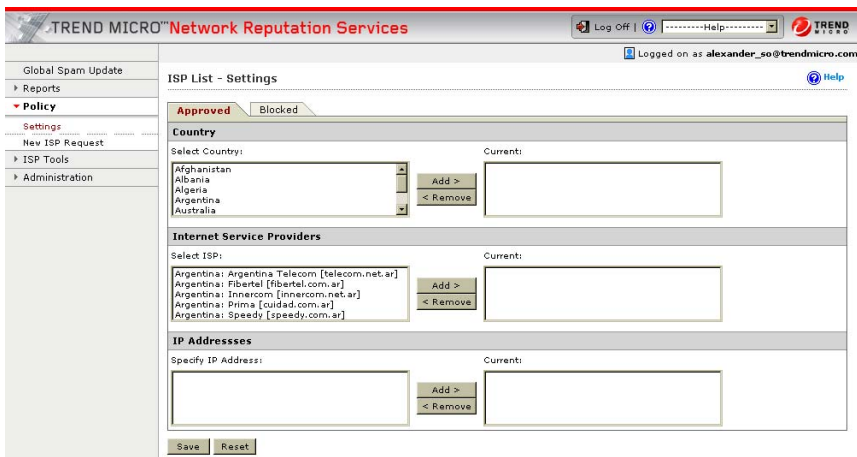
© Copyright 2006, 2007 Trend Micro Incorporated. All rights reserved.

FIGURE 3-6 ERS Daily Botnet report page

## Policy

The Policy section allows you to create or manage Approved Sender IP and Blocked Sender IP lists. You may define your Approved Senders by individual IP address and Common InterDomain Routing (CIDR), by Country as selected from the provided drop-down list, or by Internet Service Provider (ISP) as selected from the provided drop-down list.

The IP addresses that correspond to either the Country or ISP selections have been predetermined by Trend Micro to assist you in customizing the service to your unique environment.



**FIGURE 3-7** ERS Policy > Settings screen

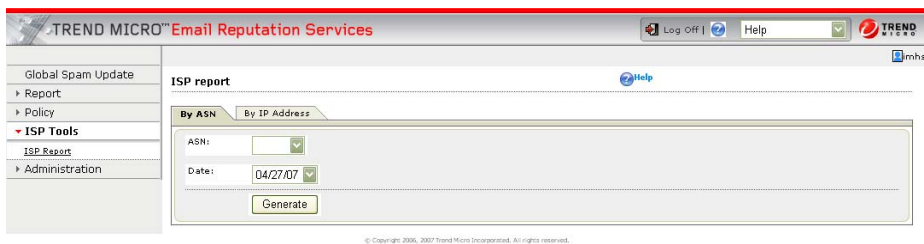
**Note:** By using the Approved Sender IP lists you are only bypassing the IP-level filtering of ERS. The Approved Sender lists are not applied to your MTA. Your MTA will process these messages and apply any filtering and policies as configured. Additional Approved Sender lists will need to be maintained by the MTA.

## ISP Tools — ISP Report

ISP accounts may obtain reports about spam and botnet traffic related to the servers within their internet address space. This report generation page allows you to generate reports based on an ASN (Autonomous System Number) or an IP address block within your allocated network space.

### ASN Report

To generate an ASN report that you can download first select the ASN of interest. Then select the date to report. Click the Generate button and a report will be generated. Click on the Download link that will appear after you click the Generate button and you will be able to download the generated report.



**FIGURE 3-8** ISP Report — ASN Report

### IP Report

To generate an IP address report that you will see within your web browser first select the IP address block desired. Then specify the start and end dates for your report and click the Generate button. A report will then be displayed at the bottom of the page.

A red robot icon within the report table indicates the presence of spamming activity for that address. Click on the robot to see a more detailed report. A single dash (-) character indicates that no spam activity was detected during the dates specified.

The detailed report that you see when you click on a red robot icon will also allow you to view a sample of a spam message sent via a server within the IP address block. The message is sanitized by Trend Micro in order to protect innocent spam victims.



**FIGURE 3-9** ISP Report — IP Report

## Administration

In the Administration section, only the system password modification feature is available.

### Changing the System Password

The console logon requires a password of between eight and thirty-two characters. Trend Micro strongly recommends using passwords that contain multiple character types (a mix of letters, numbers, and other characters) that are not part of a recognizable format (for instance, do not use your birthday, license number, etc.)



**FIGURE 3-10** ERS Administration > Change Password screen

**Note:** Super admin-level users will see three more menu items that are not displayed in Figure 3-10.

#### To change your password:

1. Type your current/old password.
2. Type your new password.
3. Confirm your new password.
4. Click **Save**.

## Valid Mail Server Administration

This page allows you to add or modify company domain and mail server data. If the form is blank then it is ready to record information about a new company. You must provide a name of the company and select the country in which the company headquarters is located. Please also provide the email address of someone at the company whom we can contact in the event that we need to validate any of the data provided.

If your company is an Internet Service Provider (ISP) then specify that company type. For very small companies owned by an individual you should select the Individual type. For all other companies select Corporation as the company type.

When you have filled in the form click the Submit button. The page will change to include form elements for managing domains and mail servers. You may now add domain names and the IP addresses of validated email servers owned by your company into the system. NOte: The IP addresses may be entered in CIDR format. So if you have all of your mail servers within a block of IP addresses then you can specify a CIDR format address that includes all of them. (CIDR format examples are: 10.0/16, 164.38.2/24, 192.168.1.45/32)

### **Adding Company Domains**

Just below the company information you may specify the names of domains owned by the company (if any). If your company owns no domains simply leave this section blank.

### **Deleting Domains**

If you wish to delete a domain (perhaps you typed the name wrong or perhaps your company has released an old domain name) simply select one or more domain names from the list by clicking on the checkbox next to the name and then click the Delete button for the list. To select all of the domains for deletion click the checkbox at the top of the checkbox column.

The screenshot shows the Trend Micro Email Reputation Services Administration Console. The page title is "TREND MICRO™ Email Reputation Services". The navigation menu on the left includes: Global Spam Update, Report, Policy, ISP Tools, Administration (selected), Change Password, Change Username, Change Activation Code, and Valid Mail Servers. The main content area is titled "Add Company" and contains the following form fields:

- Company Name:
- Administrative Contact Email:
- Company Headquarters Country:
- Company Type:

Below the form fields, there is a warning message: "In order to register valid servers for your company you must first provide information about your company. After you have completed this form you will be able to add information about your servers." At the bottom of the form is an "Add Company" button. The footer of the page reads: "© Copyright 2006, 2007 Trend Micro Incorporated. All rights reserved."

**FIGURE 3-11 Valid Mail Servers — Add Company**

## Adding Company Mail Servers

At the bottom of the block for mail servers you will see an empty text entry block that allows you to add a mail server. After adding one you will then see the new entry in the mail server list.

## Deleting Mail Servers

You may delete one or many email servers at a time. Click on the checkbox next to each server that you wish to delete and click the Delete button for the list. To select all of the servers click the checkbox at the top of the checkbox column.

If you need to modify a mail server or domain value then delete the old one and add the correct value. (See Figure 3-12)

**Update Mail Servers**

Company Name:

Administrative Contact Email:

Company Headquarters Country:

Company Type:

Domain name:

<input type="checkbox"/>	Domain Name	Status	Created
<input type="checkbox"/>	trendmicro.com	Pending	2007-04-13 15:43:05.099709-07
<input type="checkbox"/>	cup.us.trendmicro.com	Pending	2007-04-13 18:05:57.355021-07
<input type="checkbox"/>	us.trendmicro.com	Pending	2007-04-13 18:05:46.995792-07

Server IP Address:

<input type="checkbox"/>	IP Address	Status	Created
<input type="checkbox"/>	65.36.255.250	Pending	2007-04-13 15:42:54.223389
<input type="checkbox"/>	8.10.161.0/24	Pending	2007-04-13 16:01:36.829364
<input type="checkbox"/>	12.3.196.1	Pending	2007-04-13 16:13:20.935971
<input type="checkbox"/>	216.99.131.5	Accepted	2007-04-12 08:30:03.06359
<input checked="" type="checkbox"/>	216.99.131.6	Accepted	2007-04-12 08:30:22.86908
<input type="checkbox"/>	216.99.131.7	Accepted	2007-04-12 08:31:18.111503
<input type="checkbox"/>	216.99.131.8	Accepted	2007-04-12 08:32:21.521752

© Copyright 2006, 2007 Trend Micro Incorporated. All rights reserved.

**FIGURE 3-12 Valid Mail Servers — Update Mail Servers**

# Contact Information and Web-based Resources

This chapter provides information to optimize the ERS performance and get further assistance with any technical support questions you may have.

Topics in this chapter include:

- Contacting technical support
- Submitting suspicious files to Trend Micro for analysis
- Web-based resources

## Contacting Technical Support

Trend Micro offers extensive online help for ERS accounts through the administrative graphical user interface (GUI).

In addition, free support assistance for setup, configuration, and service usability is available as follows:

In the United States, Trend Micro representatives can be reached via phone, fax, or email. Our Web site and email addresses follow:

<http://www.trendmicro.com>  
[http://esupport.trendmicro.com/  
support@trendmicro.com](http://esupport.trendmicro.com/support@trendmicro.com)

Support business hours: 24 x 7

Global support phone numbers:

United States: 1(877)TREND-07 (or +1-877-873-6307)

Australia: 1 800 624 930

New Zealand: 0 800 450 553

Global support email address:

[ERS\\_Support@trendmicro.com](mailto:ERS_Support@trendmicro.com)

Please provide the following in your correspondence:

Company name

Administrator account name (only the account user name; do not send your password in an email)

Contact information:

Name

Email address (if different)

A brief description of your issue

## General Contact Information

General US phone and fax numbers follow:


Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Our US headquarters is located in the heart of Silicon Valley:

Trend Micro, Inc.  
10101 N. De Anza Blvd.  
Cupertino, CA 95014

## Supported Performance Levels

Trend Micro provides the following levels of performance for ERS. 

### Service Availability

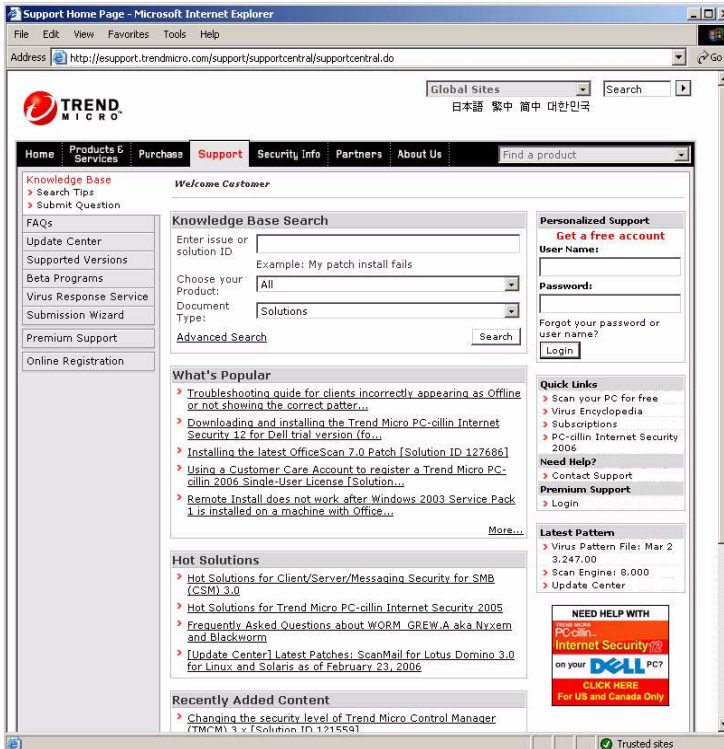
Scheduled downtime for ongoing maintenance may occur from time to time with at least 24 hours written notification provided. In the event of unscheduled downtime, no less than 99.99 percent availability is guaranteed on an annual basis.

### Email Delivery

Delivery is guaranteed even when your mail server is temporarily unavailable. The service continues to scan and process email in the event of downstream disaster recovery with valid messages stored for up to five days, depending on volume. Once your local email servers are available, email is delivered with intelligent flow control to ensure downstream manageability, avoiding unnecessary flooding of downstream resources.

## Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do to. New solutions are added daily.



**FIGURE A-1** Trend Micro Technical Support site

Also available in Knowledge Base are product FAQs, hot tips, preventive antivirus advice, and regional contact information for support and sales.

<http://esupport.trendmicro.com/>

And, if you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 24 hours or less.

## Sending Suspicious Code to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

<http://subwiz.trendmicro.com/SubWiz>

Click the “Submit a suspicious file/undetected virus” link.

**FIGURE A-2** Submission Wizard screen

You are prompted to supply the following information:

- **Email:** Your email address where you would like to receive a response from the antivirus team.
- **Product:** The product you are currently using. If you are using multiple Trend Micro products, select the product that has the most effect on the problem submitted, or the product that is most commonly in use.
- **Number of Infected Seats:** The number of users in your organization that are infected.
- **Upload File:** Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word “virus” as the password—then select the protected zip file in the **Upload File** field.
- **Description:** Please include a brief description of the symptoms you are experiencing. Our team of virus engineers will “dissect” the file to identify and characterize any risks it may contain and return the cleaned file to you, usually within 48 hours.

---

**Note:** Submissions made via the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

---

When you click **Next**, an acknowledgement screen displays. This screen also displays a Tracking Number for the problem you submitted.

If you prefer to communicate by email, send a query to the following address:

`virusresponse@trendmicro.com`

In the United States, you can also call the following toll-free telephone number:

(877) TRENDAY, or 877-873-6328

## TrendLabs

TrendLabs is Trend Micro’s global infrastructure of antivirus research and product support centers that provide customers with up-to-the minute security information.

The “virus doctors” at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging risks. The daily

culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA.

## Security Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

<http://www.trendmicro.com/vinfo/>

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of risks expected to trigger in the current week, and describes the 10 most prevalent risks around the globe for the current week
- View a Virus Map of the top 10 risks around the globe

### Virus Map

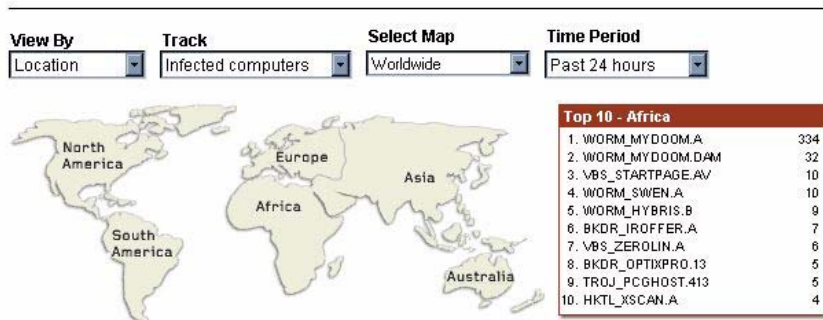


FIGURE A-3 Trend Micro World Virus Tracking Program virus map

- Consult the Virus Encyclopedia, a compilation of known risks including risk rating, symptoms of infection, susceptible platforms, damage routine, and

instructions on how to remove the risk, as well as information about computer hoaxes

- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
  - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other risks
  - The Trend Micro *Safe Computing Guide*
  - A description of risk ratings to help you understand the damage potential for a risk rated Very Low or Low vs. Medium or High risk
  - A glossary of virus and other security risk terminology
- Download comprehensive industry white papers

The screenshot shows the Trend Micro Security Information page. The main content area features a 'MALWARE ALERT' for WORM\_MYTOB.AR, described as a medium risk alert for all users. It lists aliases and provides a resolution to download virus pattern file 2.651.00. Below this, a table lists several other malware advisories.

MALWARE NAME	RISK RATING	ADVISORY DATE	PATTERN FILE
TROJ_BAGLE.AR	Low	May 31, 2005	2.652.01 (CPR)
WORM_MYTOB.BI	Medium	May 31, 2005	2.651.00
WORM_ANTIMAN.D	Low	May 30, 2005	2.650.05 (CPR)
WORM_MYTOB.AR	Medium	May 29, 2005	2.649.00
VBS_RUNEXPLT.C	Low	May 28, 2005	2.646.03 (CPR)
BKDR_TYUS.J	Low	May 28, 2005	2.646.10 (CPR)
WORM_MYTOB.EC	Low	May 26, 2005	2.646.01 (CPR)
TROJ_DLOADR.OU	Low	May 26, 2005	2.644.01 (CPR)
WORM_KELVIN.BE	Low	May 26, 2005	2.645.00
WORM_WURMARK.M	Low	May 23, 2005	2.640.10 (CPR)

FIGURE A-4 Trend Micro Security Information screen

- Subscribe, free, to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Webmasters



# Index

## C

Contact  
    general information A-3

## E

EICAR test file A-8  
Email delivery A-3

## G

Getting started 2-2  
Glossary A-8

## K

Knowledge Base A-4  
    URL A-6

## P

Product maintenance A-7

## R

Risk ratings A-8

## S

Security Information Center A-7–A-8  
Service availability A-3  
Suspicious code A-5  
    how to submit A-5  
Suspicious files A-1, A-5

## T

Technical support A-1  
    contacting A-2  
Trend Micro  
    contact information A-3  
TrendLabs A-6

## U

URLs  
    Knowledge Base A-2, A-4  
    Security Information Center A-7

## V

Virus alert service A-9

Virus doctors-see TrendLabs A-6  
Virus Encyclopedia A-7  
Virus Map A-7  
Virus Primer A-8  
Virus tracking  
    global A-7

## W

Web-based resources A-1  
Weekly virus report A-7  
White papers A-8  
World Virus Tracking A-7

