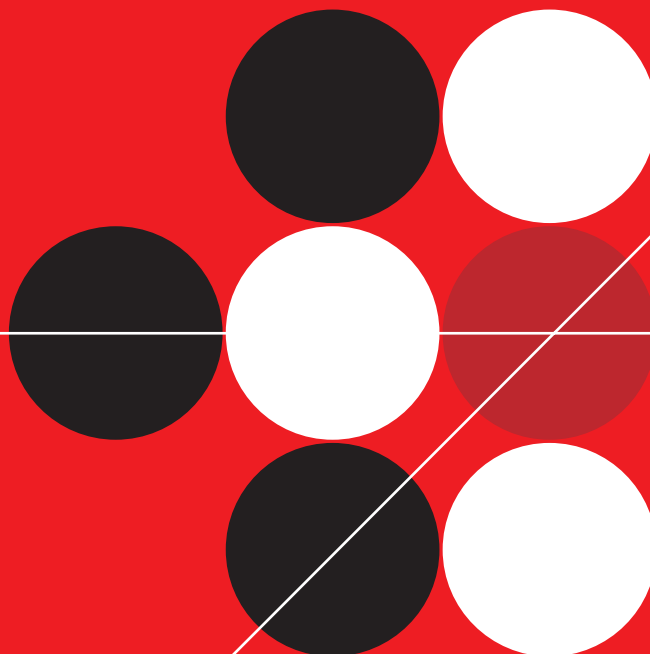


TREND MICRO™

Email Reputation Services

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.

Release Date: November 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

ProductNameVariable Documentation	iv
Audience	iv
Document Conventions	v

Chapter 1: Introducing ERS

Minimum Requirements	1-2
About Email Reputation Services (ERS)	1-2
ERS Overview	1-2
Types of ERS Service	1-2
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

Chapter 2: Getting Started with ERS

Configuring Email Reputation Services	2-2
Signing up for Service and Obtaining Service Activation Code	2-2
Trial Service	2-2
Full Service	2-2
Configuring Your MTA	2-3
Testing Your MTA Server	2-4
Creating an Account for the ERS Console	2-5

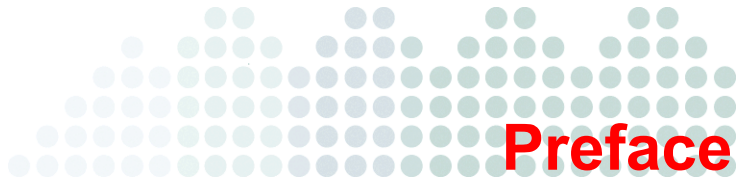
Chapter 3: Using the Administration Console

Logging on to the Administration Console	3-2
Getting Help with the Administration Console	3-2
Global Spam Update	3-3

ISP Spam Statistics	3-3
Total Spam Volume Calculation	3-4
Using Reports	3-5
Percentage Queries Report	3-5
Hourly and Daily Reports	3-6
Botnet Reports	3-7
Managing the Policy	3-9
Approved and Blocked Senders	3-9
Using the Dynamic Reputation Slider	3-10
Enabling Standard Service Settings	3-11
Enabling ERS Standard Service Database Options	3-12
Using ISP Tools: ISP Report	3-13
Report by ASN	3-13
Report by IP Address	3-14
Administration	3-15
Changing the System Password and Username	3-15
Changing the Activation Code	3-16
Valid Email Server Administration	3-16
Adding Company Domains	3-17
Adding Company Email Servers	3-17

Appendix A: Contact Information and Web-based Resources

Contacting Technical Support	A-2
Supported Performance Levels	A-2
Service Availability	A-2
Email Delivery	A-2
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 (ERS) Getting Started Guide*. The guide introduces the main features of the service and configuration instructions for your production environment. Please read through this guide prior to configuring the service.

This preface covers the following:

- [ProductNameVariable Documentation on page iv](#)
- [Audience on page iv](#)
- [Document Conventions on page v](#)

ProductNameVariable Documentation

The Product Long Name Variable (<Product Acronym>) 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 <Product Acronym> 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)

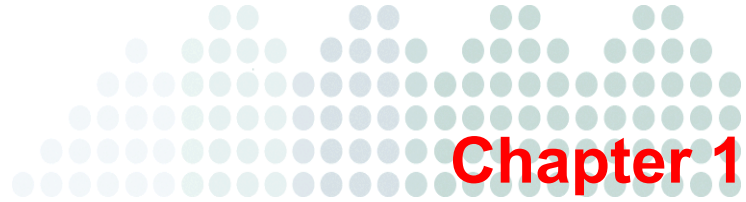
Note: Knowledge about configuring an MTA to make DNS RBL query is essential.

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 <Product Acronym> 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, helping protect businesses against spam, viruses, and inappropriate content before they reach your network.

This chapter covers the following:

- [About Email Reputation Services \(ERS\) on page 1-2](#)
- [Minimum Requirements on page 1-2](#)
- [How ERS Works on page 1-6](#)

Minimum Requirements

To use ERS, use one of the following browsers:

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

About Email Reputation Services (ERS)

As the first line of defense, Trend Micro™ Email Reputation Services (ERS) helps stop more than 80% of spam before it can flood your network, overload email gateway security, and burden your system resources.

ERS Overview

When your email server accepts an initial connection from another email server, your email server records the IP address of the computer requesting the connection. Your email server then queries its DNS server, which in turn queries the Reputation database(s) to determine if there is a record for the IP address of the requesting computer.

If the host is listed in a database, ERS recommends an appropriate action. You can also customize actions.

Types of ERS Service

Trend Micro offers two levels of ERS service:

- **Trend Micro Email Reputation Services Standard**—Blocks spam by validating requesting IP addresses against the Trend Micro reputation database, powered by Trend Micro Threat Prevention Network.

This ever-expanding database currently contains over a billion IP addresses with reputation ratings based on spamming activity. Trend Micro's spam investigators continuously review and update these ratings to ensure accuracy.

ERS Standard Service is a DNS single-query-based service. Your designated email server makes a DNS query to the standard reputation database server whenever an incoming email 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 email. Trend Micro recommends that you block, not receive, any email from an IP address that is included on the standard reputation database.

- **Trend Micro Email Reputation Services Advanced**— Identifies and stops sources of spam while they are in the process of sending millions of messages. This is a dynamic, real-time anti-spam solution. To achieve this, our team of spam experts along with our network of automated expert systems, continuously monitor network and traffic patterns and immediately update the dynamic reputation database as new spam sources emerge, often within minutes of the first sign of spam. As evidence of spam activity ceases, the dynamic reputation database is updated accordingly.

Like ERS Standard, ERS Advanced is a DNS query-based service, but two queries can be made to two different databases: the standard reputation database and the dynamic reputation database (a database updated dynamically in real-time). These two databases have distinct entries (no overlapping IP addresses), allowing Trend Micro to maintain a highly efficient and effective database that can quickly respond to highly dynamic sources of spam.

ERS Advanced Service has blocked more than 80% of total incoming connections in customer networks. Results will vary depending on how much of your incoming email 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/.

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. An IP address receives a reputation assignment if it:

- Sent spam or in some way has supported the sending of spam (for example, offering services to spammers or allowing their resources to be used by those who send spam).
- Is an unsecured email server (“open relay”) that has been used to send spam
- Is an unsecured port on a machine (“open proxy”) that has been used to send spam
- Is a dynamically assigned address that should not be used as an email server

Before processing an IP address, the Threat Prevention Network categorizes it according to careful guidelines. 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 includes samples of the actual spam received from the IP address, the history of spamming behavior, a record of any correspondence regarding mediation, any resolution of issues, and other related information. For dynamically assigned IP addresses that were submitted to the standard reputation database by the ISP, the reputation record will include submission dates and any limitations that the ISP placed upon it.

The reputation of an IP address can be viewed by using the IP Lookup Tool found on:

- The MAPS Web site: www.mail-abuse.com/cgi-bin/lookup
- The Trend Micro Security Services Web site: <https://www.securecloud.com>

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 an email server accepts the initial connection from another email server, it records the IP address of the machine requesting the connection. The receiving email server then queries its DNS server, which in turn queries the Reputation DNS server to determine if there is a record for that IP address.

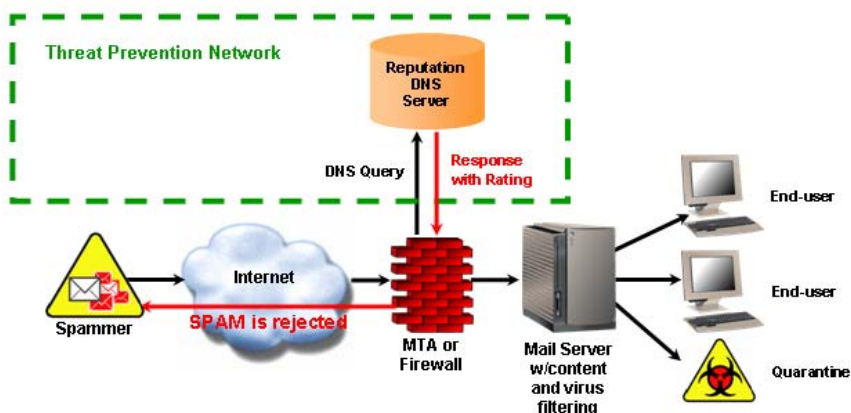


FIGURE 1-1 Threat Prevention Network Workflow

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 email 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 email server returning a '450' error, or 'temporary failure' of the requested connection. Listings in this database are occasionally legitimate email servers that have compromised hosts behind them that are temporarily sending spam. If the connection request is from a legitimate email server it will re-queue and try

again later, causing a delay in email delivery until the listing expires but not blocking email.

Depending on your email 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 email infrastructure. Keeping unwanted spam out of the infrastructure means that valuable bandwidth, processing and storage resources are not wasted.

Blocking Connections vs. Messages

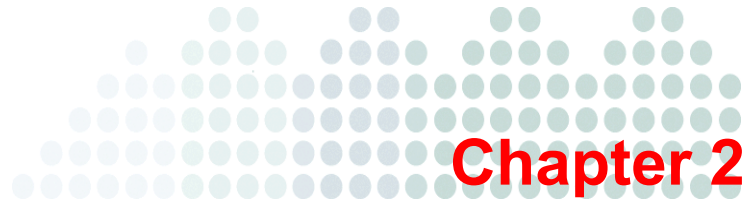
Our customers find that adding ERS to their anti-spam solutions has an exponential impact on offloading existing filtering solutions. What can appear to be only a small increase in blocked connections can translate into a large reduction of actual messages entering the filtering portion of their email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

It is far more efficient to reject spam at the connection level rather than take each message through full anti-spam scanning:

TABLE 1-1. Connection Blocking and Scanning Requirements

CONNECTION BLOCKING REQUIREMENTS	SCANNING EACH MESSAGE REQUIREMENTS
The initial portion of the SMTP handshake	The full SMTP-handshake
A DNS query	Complete message parsing, putting strains on computers that run anti-spam solutions



Getting Started with ERS

This chapter covers the following:

- [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

ERS is most effective when it is the first line of defense in your messaging infrastructure. Trend Micro recommends that you remove any other DNS blocking techniques after you enable ERS.

To enable and configure ERS see the following:

1. Step 1—[Signing up for Service and Obtaining Service Activation Code on page 2-2](#)
2. Step 2—[Configuring Your MTA on page 2-3](#)
3. Step 3—[Creating an Account for the ERS Console on page 2-5](#)

Signing up for Service and Obtaining Service Activation Code

Sign up for a trial evaluation or purchase the full service. If you sign up for a trial, you need to complete the request form appropriate for the service level you wish to evaluate. See the following Web site:

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

Trial Service

After you register for the trial service, Trend Micro sends you an Activation Code email with instructions for configuring your MTA. This Activation Code will only be good for the length of the evaluation. You need to obtain a new Activation Code when you purchase the service.

Full Service

If you purchase the full service, Trend Micro provides you with instructions on creating a customer account. After you create the account, Trend Micro sends you an Activation Code email with an Activation Code.

The Activation Code allows you access to only the level of service to which you are registered (Standard or Advanced).

Note: Please note that the Activation Code for Email Reputation Services Advanced includes access to Email Reputation Services Standard which is a sub-component.

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 type of Email Reputation Service to which you subscribed:

- **ERS Standard**—Reject connections with a 550 level error code (connection refused). Your MTA returns this error code to the server initiating the connection because the IP address is in the Standard Reputation database as a known spammer.
- **ERS Advanced**—Configure your MTA to make two DNS queries. If the MTA does not receive a positive response from the first query to the **standard** reputation database, it needs to make a second query to the **dynamic** reputation database. Your MTA should return a temporarily deny connection 450 level error code (server temporarily unavailable, please retry), when a positive response is received from this database.

Legitimate email servers that may have compromised hosts behind them temporarily sending spam may be listed in the dynamic reputation database. If the connection request is from a legitimate email 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 email.

Some servers may have additional options for handling questionable IP connections. These options include throttling or routing messages for more detailed scanning.

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

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

ERS 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. Refer to your product's manuals and/or technical support organization for detailed configuration and set-up options.

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

Testing Your MTA Server

Once you configure your MTA server, send an email to ers_support@trendmicro.com to request an email message that tests if your mail server is properly configured to use the services.

Tip: Trend Micro recommends using any reporting features that your MTA products offer to track the effectiveness of your ERS implementation.

Creating an Account for the ERS Console

To create an account:

1. Open your browser to the following URL:
`https://ers.trendmicro.com/index.php`
The ERS login screen appears.
2. On the Click **Register a New Account**.

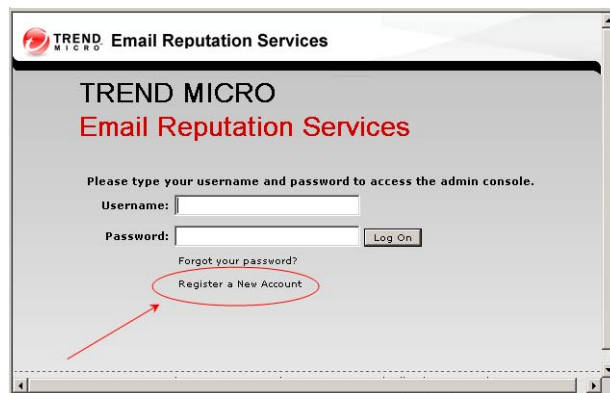


FIGURE 2-2 ERS Login Screen

3. Complete the **New Account Request** form:
 - **Username**
 - **Email**
 - **Activation Code**

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

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!

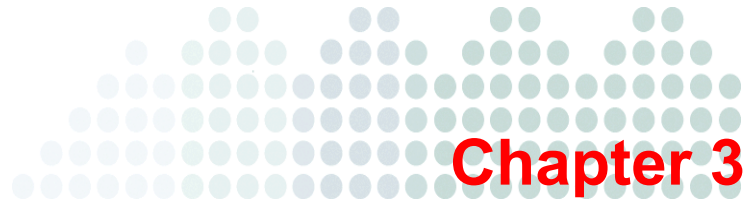
Username:

Email:

Activation Code:

FIGURE 2-3 ERS New Account Request Screen

4. Click **Submit**. Trend Micro sends you an email with a password.



Using the Administration Console

After you create an ERS account, you will receive an email that provides you with account details and a temporary password. Log on the administration console and begin configuring your settings.

This chapter covers the following:

- [Logging on to the Administration Console on page 3-2](#)
- [Global Spam Update on page 3-3](#)
- [Using Reports on page 3-5](#)
- [Managing the Policy on page 3-9](#)
- [Using ISP Tools: ISP Report on page 3-13](#)
- [Administration on page 3-15](#)

Logging on to the Administration Console

To log on to the console:

1. Open your browser to the following URL:

<https://www.securecloud.com>

The ERS login is located in the top-right corner of the screen.

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

Note: After you log in for the first time, Trend Micro recommends changing your password. (See the [Administration on page 3-15](#).)

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 help icon (🔍) near the upper-right corner of each screen.

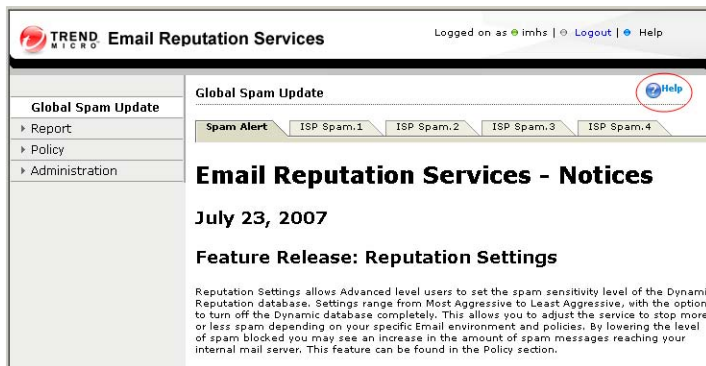


FIGURE 3-4 ERS online help access icon

Global Spam Update

After you log on the console, the Spam Alert screen appears. The Spam Alert screen, which is updated regularly, might show any of the following:

- A brief overview and discussion of current spamming tactics
- How spammers are deploying new tactics and how spam has been designed to get through systems
- How Trend Micro is responding to these new threats
- Global spam statistics, such as Internet spam levels and blocking percentages. Use these to compare how effective your spam protection is.

ISP Spam Statistics

The spam statistics screen ranks ISPs based on the amount of spam they receive. The calculation is based on total spam volume (see below for calculation information) that an ISP receives for a week. The following colors indicate spam change over the week:

- Red—An increase
- Yellow—No change
- Green—A decrease

The following items are also shown:

- **ASN**—The Autonomous System Number (ASN) is a globally unique identifier for a group of IP networks having a single, clearly defined routing policy that is run by one or more network operators.
- **ISP Name**—The registered name for a particular ASN. Some ISPs may have multiple ASNs and therefore appear more than once in the table. At the same time, some ASNs may have multiple registered ISPs.
- **Spam Volume (24 hours)**—The estimated total spam that has been sent during the previous 24 hours. This is a rolling number that is updated every hour.
- **Botnet Activity**—An indication of how active botnets are within a specific ISP. Botnets are groups of infected computers that are controlled by a spammer from a central location. They are the largest source of spam on the Internet today. This number indicates the percentage change in the number of bots from the previous hour. To see botnet activity, you must add your email servers to the Valid Mail Servers list (see [Adding Company Email Servers on page 3-17](#)).

Total Spam Volume Calculation

Trend Micro calculates the spam volume for each ISP using a Base Volume Number, which is derived from the total connection requests from known spam sources that Trend Micro and ERS customers receive. The final Spam Volume per ISP results from the extrapolation of the Base Volume.

Trend Micro uses a combination of multipliers upon which to base the extrapolation. The multipliers are based on the following:

- **Connections versus Spam Messages**—In order to maximize delivery potential, spammers will attempt to deliver more than one spam message per SMTP connection. Trend Micro measures connections and applies a MULTIPLIER of 5 to the total number of spam connections.
- **Caching**—A customer's server does not query every IP connection requested by the customer MTA because of local caching, which can distort the statistics. Trend Micro applies a MULTIPLIER of 2 to offset the affect of server caching.
- **Global View**—Although Trend has many customers, the customer base does not represent every email system in the world. Based on the size of our customer base and estimated total volume of email worldwide, Trend Micro applies a MULTIPLIER of 9 to give a global view of how much spam is being sent by each ISP.

With thousands of active customers, including some of the largest ISPs in the world, the Base Volume Number gives us a very broad view across the spam landscape, and the extrapolation allows us to estimate the global magnitude of the spam problem.

We will continue to adjust these multipliers to represent our best estimate of the true volume of spam. Naturally, each ISP can accurately count their true spam volume simply by incrementing their outbound connections.

Using Reports

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

You will also be able to see a daily botnet activity report for each mail server that you add to the Valid Mail Servers list (See the [Administration on page 3-15](#)).

The color of the bars in the graph depends on the service level.

- **Blue**—Corresponds to the initial query to the standard reputation database. If you subscribed to the standard ERS service (Trend Micro Standard Service), only a blue graph appears.
- **Orange**—Corresponds to the second query to the dynamic reputation database. If you subscribed to the ERS Advanced service, orange bars might appear on top of the blue bars. The blue portion corresponds to the initial query to the standard reputation database, and the orange portion refers to the second query to the dynamic reputation database.

Percentage Queries Report

The Percentage Queries report shows the percentage of queries that returned an IP address match, which indicates that a sender trying to establish a connection with your email server is a known spammer. The reports are based on connections, not individual spam messages.

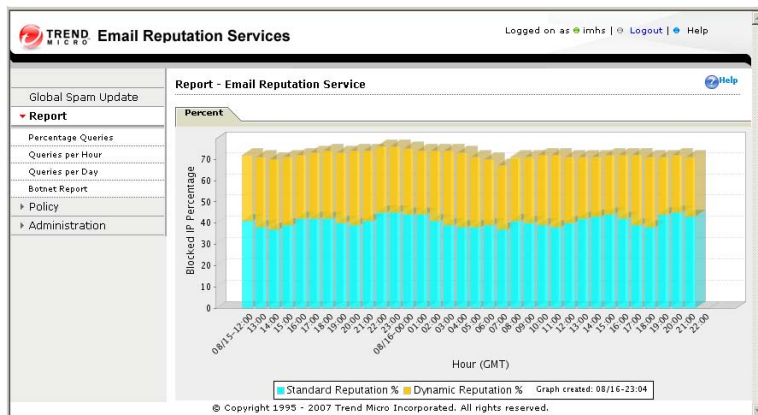


FIGURE 3-5 ERS report — Percent Listed screen

Note: This report shows only a portion of the activity happening at your gateway, depending on the level of caching you set up on your system.

Hourly and Daily Reports

The Queries per Hour and Queries per Day reports show how many times your email server queried the reputation database.

To view queries for the standard reputation database, click the **ERS Standard** tab.

To view queries for the dynamic reputation database, click the **ERS Advanced** tab. This tab does not appear if you did not subscribe to the advanced service.

Note: The reports show only a portion of the activity happening at your gateway, depending on the level of caching you set up on your system.

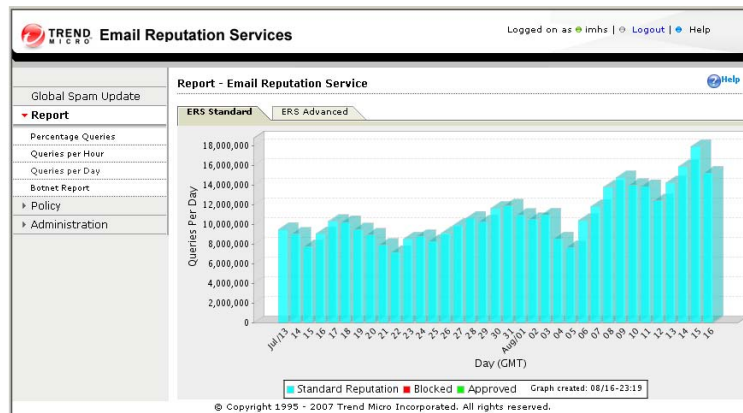


FIGURE 3-6 ERS Daily query report page

Botnet Reports

The Botnet report provides a quick summary of spam activity originating from the servers that you listed as valid mail servers. If there was any spam activity for any of the IP addresses that you specified, a red robot icon (🤖) appears.

To view details about the specific spam counts, click the robot icon. A pop-up window appears showing the IP address of the email server, the date that ERS detected the spam activity, the number of spam messages that ERS detected, and the number of recipients that received spam from this botnet.

Under **Spam Sample**, click view to see a sample of the spam message that ERS detected. The sample contains certain obscured information to protect the privacy of spam recipients.

Note: An email server must be on the Valid Mail Servers list for ERS to consider it in a Botnet report (see [Valid Email Server Administration on page 3-16](#)).

TREND MICRO Email Reputation Services		Logged on as imhs Logout Help						
Global Spam Update	BOTNET Activity Help							
Report	Botnet Activity - Last 7 days							
Percentage Queries	IP Address	Today	04/25/07	04/24/07	04/23/07	04/22/07	04/21/07	04/20/07
Queries per Hour	65.36.255.250	—	—	—	—	—	—	—
Queries per Day	8.10.161.0/24							
Botnet Report	12.3.196.1	—	—	—	—	—	—	—
Policy	216.99.131.5	—	—	—	—	—	—	—
Administration	216.99.131.6	—	—	—	—	—	—	—
	216.99.131.7	—	—	—	—	—	—	—
	216.99.131.8	—	—	—	—	—	—	—
© Copyright 2006, 2007 Trend Micro Incorporated. All rights reserved.								

FIGURE 3-7 ERS Daily Botnet report page

Managing the Policy

The Policy section allows you to do the following:

- Create an **Approved Sender** list—Instruct ERS to always allow email messages from certain trusted countries, ISPs, and IP addresses.
- Create a **Blocked Sender** list—Instruct ERS to always block email messages from certain countries, ISPs, and IP addresses.
- Request that an ISP be added to the official list of ISPs.
- Adjust Dynamic Reputation settings.

You can define the lists by individual IP addresses (also in Common InterDomain Routing (CIDR) format), by Country, or Internet Service Provider (ISP).

Approved and Blocked Senders

Approved Sender lists allow messages from the approved senders to bypass IP-level filtering. The Approved Sender lists are not applied to your MTA, but you can set up additional approved or blocked senders lists or do additional filtering at your MTA. The trade-off for bypassing IP filtering is the additional resources that are needed to process, filter, and store the higher levels of spam messages that would otherwise have been blocked. When using the Approved Sender list, you may experience lower overall spam catch rates.

In the case of an Standard Reputation (RBL) service lookup, the order of the evaluation hierarchy is:

- Approved IP
- Blocked IP
- Approved ISP or ASN
- Blocked ISP or ASN
- Approved Country
- Blocked Country

For Dynamic Reputation (QIL) service lookup, the customer-defined “blocked policy lists” (IP, ISP/ASN, Country) are ignored; only the Approved lists are checked. Otherwise, the order of policy lookup (first IP, then ISP/ASN, lastly Country) is the same as for Standard Reputation (RBL) service.

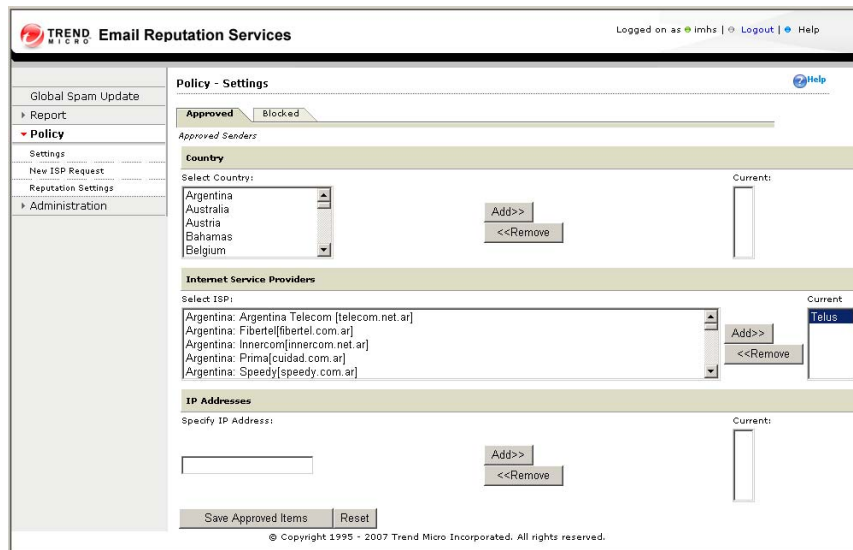


FIGURE 3-8 ERS Policy > Settings screen

Using the Dynamic Reputation Slider

If you subscribed to ERS Advanced, you can adjust how aggressively ERS blocks email connections:

- **More aggressive**—If too much spam is reaching your network, select a more aggressive setting. However, this might increase false positives by blocking connections from legitimate email senders.
- **Less aggressive**—If legitimate email is being blocked, select a less aggressive setting.

To adjust dynamic reputation settings:

1. From the menu, choose **Policy > Reputation Settings**.
2. Move the slider to one of the following points:
 - **Level 4**—The most aggressive setting. If ERS detects even a single spam message from a sender IP address, it adds the sender address into the dynamic reputation database. The length of time that the IP address stays in the database depends on whether ERS detects additional spam from the sender.

- **Level 3:** A moderately aggressive setting. ERS allows a small volume of spam from senders with a good rating. However, if ERS detects an increase in spam beyond the allowable threshold from such a sender, it will add the sender to the dynamic reputation database. The length of time that the IP address stays in the database depends on whether ERS detects additional spam from the sender. The length of time may be extended up to maximum as in Level 4.
 - **Level 2:** A moderately tolerant settings. ERS allows a larger volume of spam from a sender with a good rating. However, if ERS detects an increase in spam above the allowable threshold from such a sender, it will add the sender to the dynamic reputation database. The length of time that the IP address stays in the database is generally shorter than the time for level 3.
 - **Level 1:** The least aggressive setting. ERS allows the same amount of spam from a sender with a good rating, as in level 2. In addition, ERS allows connections from all known valid mail servers, regardless of whether or not they send spam. The length of time that an IP address stays in the database is short, in general, than for the time in level 2.
 - **Level 0**—Turns off all queries to the dynamic reputation database.
3. Click **Save**.

Note: The default setting is level 4.

Enabling Standard Service Settings

You may enable your choice of the lists which make up the Standard Reputation database. The default setting is for all lists to be enabled. This is the most effective combination for reducing spam levels which meets most customers needs.

Customers who disable some portions of the Standard database may see an increase in the amount of spam messages that reach their internal mail server for additional content filtering.

The following feature set is available for Standard Settings:

- Customers to enable or disable the lookup of selected lists by using the checkboxes in the “Enable Standard Settings” section.
 - Check the checkbox to enable the list.

- Uncheck the checkbox to turn off the list. The ERS system will not consider that list during a lookup request.
- Advanced customers will see both the Dynamic Settings and the Enable Standard Settings sections.
- Standard customer will see only the Enable Standard Settings section.
- The Save button will save new settings.
- The Cancel button will return to last saved settings.

Enabling ERS Standard Service Database Options

Email Reputation Services Standard Service includes a database with the following four lists:

- **The Realtime Blackhole List (RBL)** is a list of IP addresses of mail servers that are known to be sources of spam.
- **The Dynamic User List (DUL)** is a list of dynamically assigned IP addresses, or those with an Acceptable Use Policy (AUP) that prohibits public mail servers. Most entries are maintained in cooperation with the ISP owning the network space. IP addresses in this list should not be sending email directly, but should be using their ISPs mail servers.
- **The Relay Spam Stopper (RSS)** is a list of IP addresses of mail servers that are open mail relays and are known to have sent spam. An open mail relay is a server that will accept mail from any user on the Internet that is addressed to any other user on the Internet, making it difficult or impossible to track spammers.
- **The Open Proxy Stopper (OPS)** is a list of IP addresses of servers that are open proxy servers and are known to have sent spam. An open proxy server is a server that will accept connections from any user on the Internet and relay them to any server on the Internet, making it difficult or impossible to track spammers.

Using ISP Tools: ISP Report

Note: This section is relevant for only ISPs with an ISP account.

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

Report by ASN

To generate a report by ASN, select the ASN of interest, and then select the date to report. Click the **Generate** button and a report will be generated. Then click on the **Download** link that will appear.

Note: If there is no reported data for the ASN, you will see a notification message but a download link will not appear.

The report shows the following:

- **IP Address**—The IP address
- **Date**—The date and time of the report
- **Spam Count**—The number of spam email for this IP address
- **RCPT Count**—The number of users that received this spam



The screenshot displays the Trend Micro Email Reputation Services Administration Console. The top navigation bar includes the Trend Micro logo, the text "Email Reputation Services", and user information: "Logged on as NRS-super | Logout | Help". A left-hand navigation menu contains links for "Global Spam Update", "Report", "Policy", "ISP Tools" (which is expanded to show "ISP Report" and "Administration"), and "Administration". The main content area is titled "ISP report" and features two tabs: "By ASN" (selected) and "By IP Address". Below the tabs are two input fields: "ASN:" and "Date:". A "Generate" button is positioned below these fields. At the bottom of the form, a small copyright notice reads: "© Copyright 1995 - 2007 Trend Micro Incorporated. All rights reserved."

FIGURE 3-9 ISP Report — ASN Report

Report by IP Address

To generate a report by IP address, select the IP address block desired, and then specify the start and end dates for the report. Click the **Generate** button. A report will appear at the bottom of the page.

The report shows the following:

- **IP Address**—The IP address
- **Date**—The date and time of the report
- **Spam Count**—The number of spam email for this IP address
- **RCPT Count**—The number of users that received this spam
- **Spam Sample**—Click the View link to see a sample.

A single dash (-) character indicates that no spam activity was detected during the dates specified.



FIGURE 3-10 ISP Report — IP Report

Administration

The Administration section allows you to do the following:

- Change the administration console username and password
- Change the activation code
- Update company information and add email servers to the Valid Mail servers list

Changing the System Password and Username

To protect your account, Trend Micro recommends changing the password regularly. You can also change the username, although do so only if necessary. The password must be between eight (8) and thirty-two (32) alphanumeric characters.

To change the password and/or username, choose **Administration > Change Password** or **Change Username** from the menu. Type the old password once, and the new password twice. To change the username, just type a new username.

FIGURE 3-11 ERS Administration > Change Password screen

Note: Super admin-level users will see three more menu items that are not displayed in [Figure 3-11](#).

Changing the Activation Code

If you receive a new Activation Code from Trend Micro, enter it on the Change Activation Code screen to upgrade, reactivate, or continue to use your service. If your new activation code validates correctly then it will be saved and used immediately.

To change your activation code, type your new activation code, and then click **Save**.



FIGURE 3-12 ERS Administration > Change Activation Code screen

Valid Email Server Administration

Use this screen to add or modify company domain and mail server data. If the form is blank, it is ready to record information about a new company.



FIGURE 3-13 Valid Email Servers — Add Company

Adding Company Domains

To add a domain, click the **Domain** tab. To remove a domain name, select the check box next to the item and click **Delete**. If your organization owns no domains, leave this section blank.

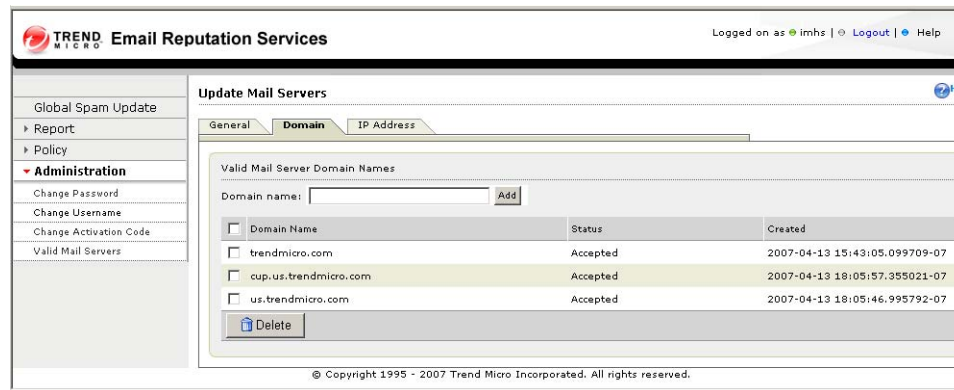


FIGURE 3-14 Valid Email Servers — Update Domains

Adding Company Email Servers

Add your email servers to the Valid Mail Server list to be able to receive Botnet activity reports for those servers (see [Botnet Reports on page 3-7](#)). To add an email server, click the **IP Addresses** tab. Type the address in the text box next to **Server IP address**, and then click **Add**. To remove an email server IP address, select the check box next to the

item and click **Delete**.



FIGURE 3-15 Valid Email Servers — Update Email 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 on page A-2](#)
- [Supported Performance Levels on page A-2](#)
- [Knowledge Base on page A-4](#)
- [Sending Suspicious Code to Trend Micro on page A-5](#)
- [TrendLabs on page A-6](#)
- [Security Information Center on page A-7](#)

Contacting Technical Support

For registered users, Trend Micro provides technical support, virus pattern downloads, and program updates for one year. Afterwards, you can purchase a maintenance renewal.

If you need help or just have a question or comment, please feel free to contact us.

Trend Micro, Inc.

10101 North De Anza Blvd.

Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales)

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

Fax: +1 (408) 257-2003

Support: <http://www.trendmicro.com/support>

Documentation: <http://www.trendmicro.com/download>

Web address: www.trendmicro.com

Email: ers_support@trendmicro.com

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 email 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.

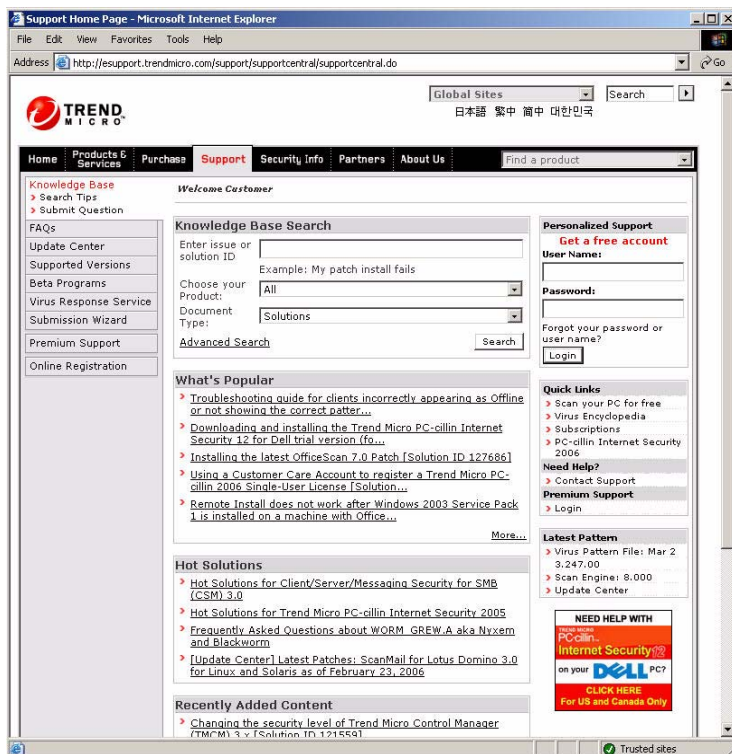


FIGURE A-1. Trend Micro Technical Support site

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.

The screenshot shows a web browser window displaying the Trend Micro Submission Wizard. The browser's address bar shows the URL: <http://subwiz.trendmicro.com/SubWiz/Undetected/malware-form.asp?TMSessionid=CB11C8EDFC764028B98C6C3F249F62D6&proc=7>. The page features the Trend Micro logo and a navigation menu with links for Home, Products, Purchase, Support, Security Info, Partners, and About Us. A left sidebar contains a Knowledge Base menu with options like Knowledge Base, FAQs, Update Center, Supported Versions, Beta Programs, Virus Response Service, Submission Wizard, Submit a Case, Case Tracking, and Submit Feedback. The main content area is titled "Submit a Suspicious File/Undetected Virus" and contains a form with the following fields: Email (text input), Product (dropdown menu), Number of Infected Seats (dropdown menu), Upload File (text input with a "Browse..." button), and Description (text area). A "Next >>" button is located at the bottom right of the form. Below the form is a disclaimer: "Disclaimer: Response time and priority case handling is based on the Customers agreed to service level (e.g. Home User, Corporate, Premium). Free service Submission Wizard may take longer. Other than for Premium Support Customers, please contact your local technical support for a faster service fee based response: <http://www.trendmicro.com/en/about/contact/overview.htm> Premium Support Customers please enter virus support case here: <https://premium.trendmicro.com/premiumsupport/en/US/PSP/login/login.asp>". The footer of the page includes the copyright notice: "Copyright 1999-2004 Trend Micro, Inc. All rights reserved. [Legal Notice](#) and [Privacy Policy](#)".

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) TRENDAV, 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

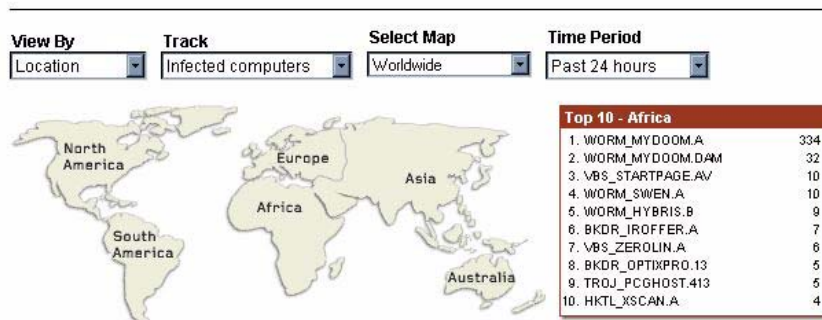


FIGURE A-3 Trend Micro World Virus Tracking Program virus map

- 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

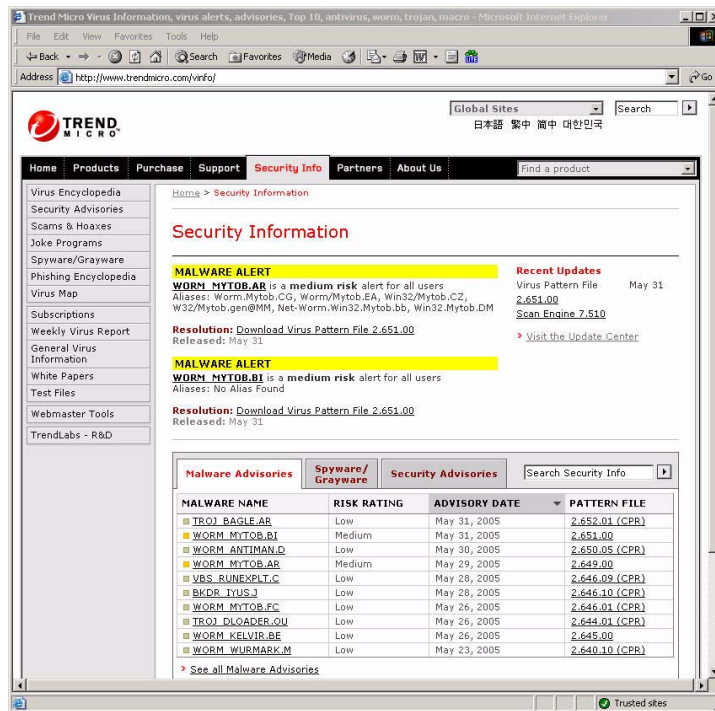


FIGURE A-4. Trend Micro Security Information screen

- 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

A

- account creation 2-5
- administration 3-15
- administration console, console 3-2
- ASN reports 3-13
- autonomous system number 3-3

B

- botnet activity 3-3

C

- connections, blocking, spam
 - blocking connections 1-7

D

- database options
 - Standard Settings 3-11
- dynamic reputation slider 3-10

E

- EICAR test file A-8
- Email delivery A-2
- email servers 3-17
- email servers, domains 3-16
- ERS
 - advanced, advanced service 1-3, 1-6
 - configuring 2-2
 - creating an account 2-5
 - how it works 1-6
 - signing up, signing up 2-2
 - standard, standard service 1-2, 1-6
 - types 1-2

F

- full service 2-2

G

- Getting started 2-2
- Glossary A-8

I

- ISP

- report 3-13
- tools 3-13

K

- Knowledge Base A-4
- URL A-6

L

- logging on 3-2

M

- MAPS 1-4
- minimum requirements 1-2
- MTA
 - configuration 2-3
 - testing the server 2-4

O

- online help, help files 3-2

P

- password, username 3-15
- policy management 3-9
- Product maintenance A-7
- product overview, ERS
 - overview 1-2

R

- reports 3-5
 - ASN 3-13
 - botnet 3-7
 - daily and hourly 3-6
 - percent listed 3-5
- reputation assignment 1-4
- requirements 1-2
- Risk ratings A-8

S

- Security Information Center A-7–A-8
- Service availability A-2
- spam
 - statistics 3-3
- spam volume 3-3

Standard Service Settings 3-11

Suspicious code A-5

 how to submit A-6

Suspicious files A-5

system requirements 1-2

T

Technical support

 contacting A-2

Threat Prevention Network 1-3

total spam volume 3-4

TrendLabs A-6

trial service 2-2

U

URLs

 Knowledge Base 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 console 2-5

Weekly virus report A-7

White papers A-8

World Virus Tracking A-7