



TESTING GUIDE
TREND MICRO™ CONTROL MANAGER™

AUGUST 2002

TREND MICRO, INC.
10101 N. DE ANZA BLVD.
CUPERTINO, CA 95014
T 800.228.5651 / 408.257.1500
F 408.257.2003
WWW.TRENDMICRO.COM

How to Test Outbreak Commander

TREND MICRO CORPORATE PROFILE

Trend Micro™ has been a pioneer in the antivirus software market since 1988, developing innovative strategies to protect information as new computing standards are adopted around the world. Trend Micro is the global leader in server-based antivirus software with a market share of more than 60% at the Internet Gateway¹. Trend Micro's antivirus products and services are designed to integrate with leading firewalls, intrusion detection systems, and other best-of-breed solutions for the complete enterprise strategy. All Trend Micro's products and services are backed by TrendLabs™, a global network of antivirus research and support centers. With over 250 engineers and antivirus specialists, TrendLabs monitors potential security threats worldwide 24x7 and develops the means to identify, detect, and eliminate new viruses and deliver prompt, effective strategies.

¹ IDC™ bulletin, 2001

SIGNIFICANT CHANGES IN THE ANTIVIRUS INDUSTRY

Blended virus threats like Nimda have become increasingly more common. A blended threat is a complex virus or worm program that targets multiple weaknesses in computer networks and is capable of doing damage in multiple ways. Unlike traditional viruses, which rely on the user to spread the infected files, blended threats use multiple distribution methods and require no human intervention to spread. According to a recent report from IDC™ titled, Worldwide Secure Content Management Software Forecast, 2002-2006: The Evolution of Antivirus, because "blended threats are designed to get past point-solution security systems, there will be a strong push towards a 'layered security' approach, which will be better able to combat blended threats." IDC also mentions that as a result of these blended threats, customers are increasingly asking for better (i.e. proactive) virus protection techniques. Updated pattern files and scan engines are no longer enough. Customers today need a strategy that can handle the complexities of this new breed of virus.

TREND MICRO'S ENTERPRISE PROTECTION STRATEGY

Today's businesses are increasingly dependent on computing environments that are both highly distributed and globally connected via the Internet. The potential benefits of migrating to a multi-platform networked architecture are substantial; in addition to streamlining operations and reducing costs, enterprises can rapidly expand business capabilities through deployment of emerging new mobile devices, Web services, and online applications.

Still, adopting new network-enabled technologies also heightens enterprise exposure to potentially crippling computer viruses and other malicious attacks. A broad range of existing security strategies help businesses guard against such common threats as Trojans, buffer overflows, and denial-of-service attacks but they do not sufficiently protect businesses from the hundreds of new threats that appear monthly.

As a result, today's connected enterprise faces a host of new security challenges. First, the complex, heterogeneous, and distributed nature of the corporate network makes it difficult to implement consistent security standards throughout the enterprise. Each new network service, device, or application that opens up remote access to the internal network creates a potential access point for computer viruses and other malicious code. And although effective at thwarting known threats, given their passive nature, most existing security products are largely incapable of proactively identifying and fending off new ones.

Trend Micro research shows that most businesses-regardless of size-have adopted a staged, seven-step process for responding to new security threats. Although some aspects of these procedures have been automated, they remain predominantly manual processes. For example,

notifying personnel of a new security threat via telephone, fax, or email; individually configuring gateway-level antivirus software settings to deter a specific threat; and consulting with management and security specialists to determine the most effective course of action are time consuming manual processes that delay taking effective action and increase an enterprise's chances of sustaining damage from an imminent attack.

Until recently, enterprises had no way to automate, much less coordinate, a successful end-to-end antivirus strategy. Today, the Trend Micro™ Enterprise Protection Strategy™ is available to help businesses manage the explosive costs of virus outbreaks, achieve rapid containment of viruses to prevent spreading throughout the network, improve visibility of attack status, and receive real-time reports on how enterprise operations are impacted.

Designed to meet enterprise demands for a comprehensive antivirus that is integrated, platform-independent, and-most importantly-capable of being centrally managed, the Trend Micro Enterprise Protection Strategy significantly eases the heavy administrative and technical burden of keeping enterprise networks secure. From enabling proactive enterprise protection to managing the damage and cleanup activities of post-attack restoration, the Trend Micro Enterprise Protection Strategy can help organizations manage the entire outbreak lifecycle.

SUGGESTED TESTING SCENARIO

Suggested Trend Micro Control Manager test bed: Pentium III with 450MHz or higher; 300MB of free hard drive space; 512MB of RAM; Windows 2000 Server or Windows NT version 4.0 build 1381 with SP6.0a; Microsoft IE 5.0 or later; Microsoft's IIS version 4.0 or later; Microsoft SQL Server 7.0 with service pack 2. Additionally, you may want to set up Trend Micro Control Manager with some servers and workstations in your east coast lab along with some servers and workstations in your west coast lab--this will enable you to effectively test the remote deployment, configuration, and management capabilities of this strategy.

Suggested InterScan Messaging Security Suite test bed: Dual PC with Pentium III 1G or faster processor; one Network Interface Card; Windows 2000 Server or Windows NT version 4.0 build 1381 with SP6.0a; 512MB RAM; 300 MB free disk space for program files with 1G - 2G recommended on high-traffic systems; Microsoft Internet Information Server must be installed to run the Web-based configuration utility.

HOW TO TEST OUTBREAK COMMANDER USING THE EICAR TEST FILE AND EICAR POLICY

This outlines the procedure for testing Outbreak Commander™, through Trend Micro™Enterprise Protection Strategy™(EPS), using the EICAR antivirus testfile. This procedure is geared for administrators using Trend Micro Control Manager.

This illustrates one method an administrator could use to respond, when configuring Outbreak Commander, upon notification of a virus outbreak from TrendLabs. Once the Outbreak Prevention Service (OPS) has been deployed the administrator can observe the behavior when an external user sends an email message with an infected attachment.

This also illustrates how Trend Micro InterScan Messaging Security Suite™ (IMSS) implements OPS through Control Manager, to isolate and quarantine the attachment, and pass its log information to Control Manager.

The log files from IMSS and Control Manager verify that the expected action was deploy and implemented e.g., removing the unwanted virus, EICAR, keeping it from spreading throughout the environment, while a pattern file and scan engine are being developed. Thus reducing the impact of the virus and minimizing the damage and associated cleanup cost.

TEST ENVIRONMENT

The following software and hardware have been used in this example:

1. Control Manager v2.1 Build GM 1100
2. InterScan Messaging Security Suite v5.1 Build 3147
3. Microsoft™ Exchange™ Server 5.5
4. Microsoft Windows 95 Inbox™ mail client - recipient's mailbox
5. Windows NT™ 4.0, Internet Explorer™ 6.0 - sender's mailbox

TESTING PROCEDURE

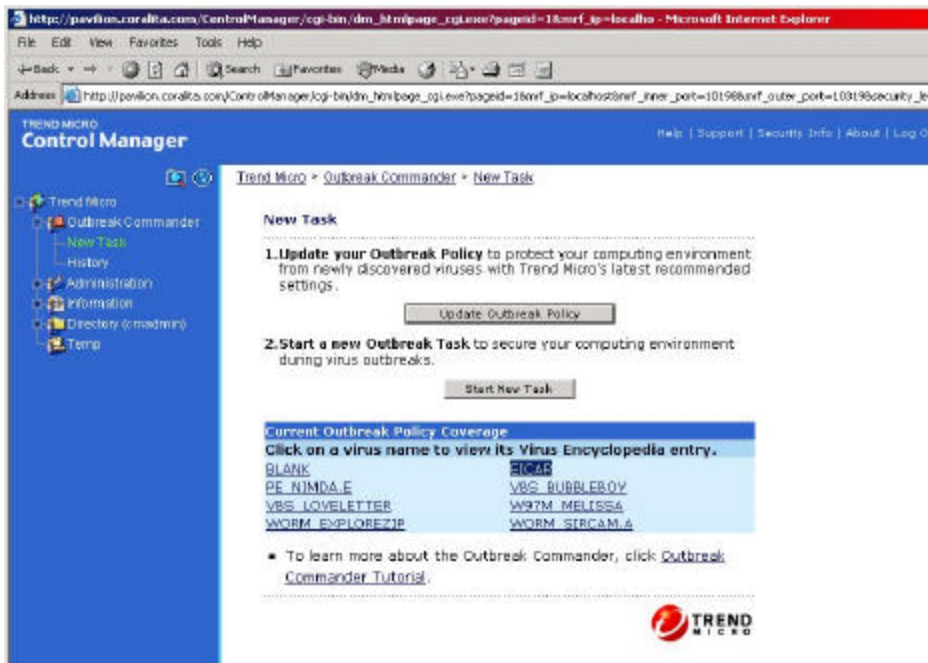
The following steps outline the procedure for verifying the Outbreak Prevention Policy using the EICAR testfile.

Update the Outbreak Policy

1. At the Control Manager Management Console, verify that the EICAR policy exists on the Control Manager server. If the EICAR policy is not available, perform the following steps to update the Outbreak Commander policy:
2. Select Outbreak Commander from the menu to display the Outbreak Commander screen.
3. Select New Task from the left-hand menu.
4. Click Update Outbreak Policy(Figure 1).

NOTE:
Download the EICAR
antivirus testfile from the
following Web sites:
Trend Micro -
<http://www.antivirus.com/vinfo/testfiles/index.htm>
EICAR -
<http://www.eicar.org>

Figure 1.
Update outbreak policy



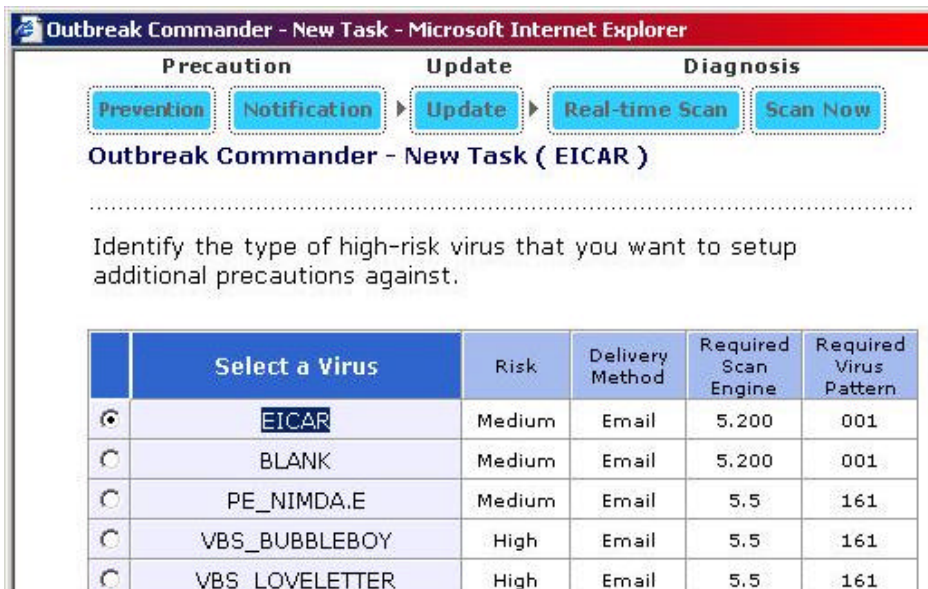
SELECT A VIRUS

Control Manager will download the outbreak policy from the Trend Micro ActiveUpdate™ server. You will perform an Outbreak Commander Task using the Outbreak Policy.

To begin a new task:

1. Click Outbreak Commander. Select New Task from the System-level menu on the left pane.
2. Click Start New Task at the New Task screen.
3. Select the EICAR virus policy(Figure 2).

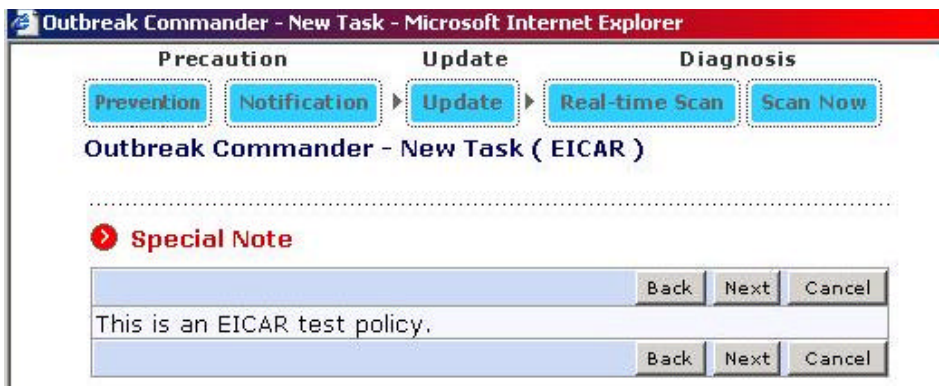
Figure 2.
Select a virus



THE SPECIAL NOTE

Read the Special Note on the EICAR virus policy (Figure 3).

Figure 3.
The Special Note

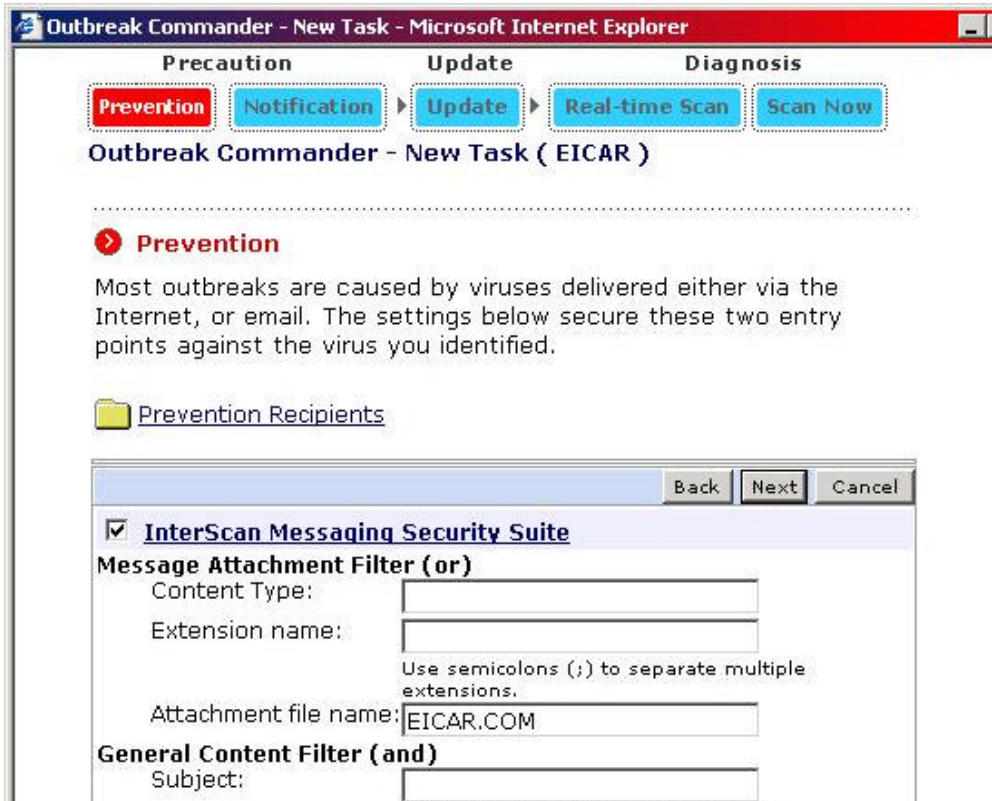


THE

PREVENTION STAGE

Select the Trend Micro product that you intend to use. In this example, IMSS has been selected (Figure 4). The attachment will have the filename and extension, EICAR.com, and will be subject to content filtering; therefore, when creating your testfile ensure the filename and extension match.

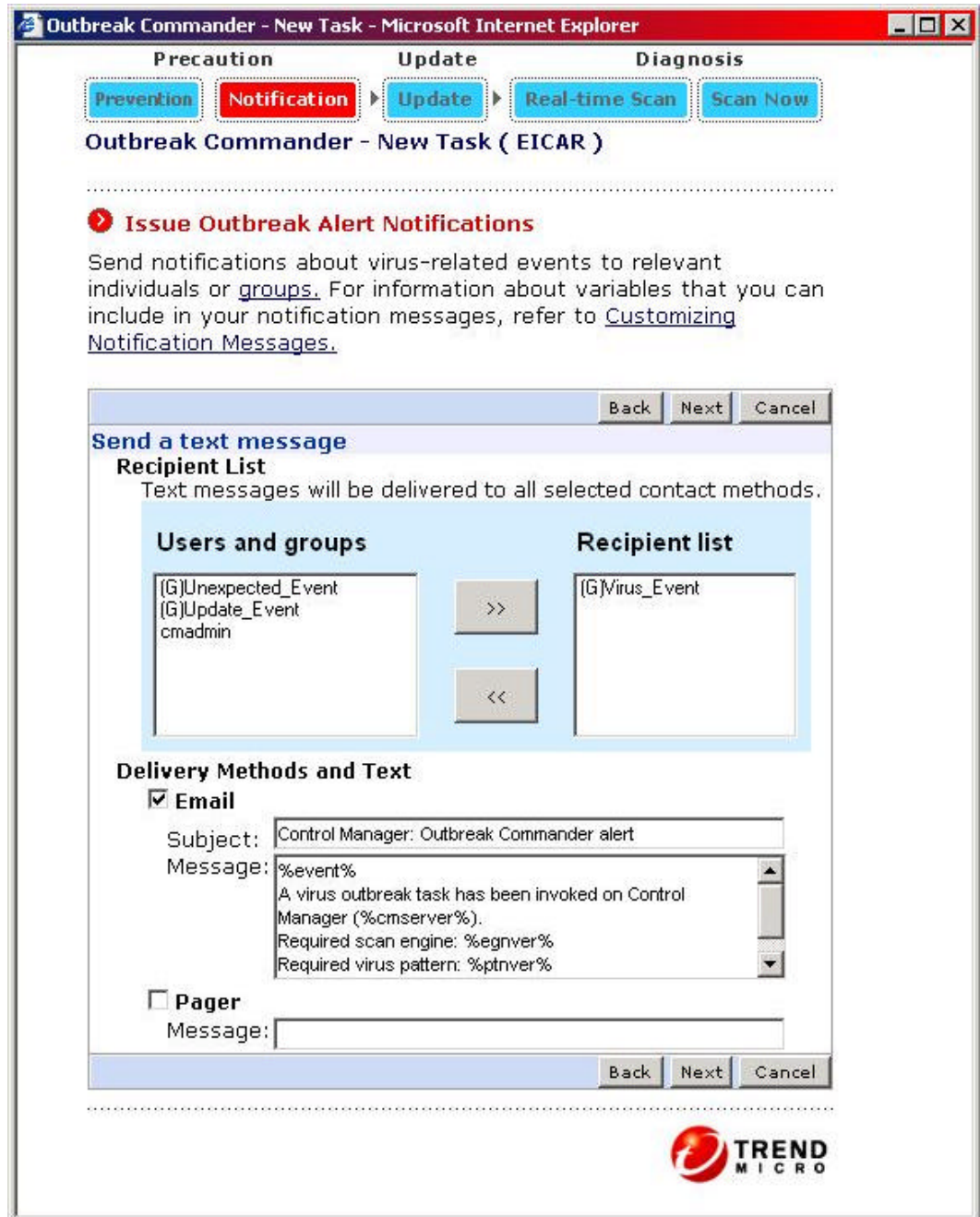
Figure 4.
Prevention Stage



THE NOTIFICATION STAGE

Choose the user profile to receive an email or pager notification. Email is easiest to test and has been used in this example (Figure 5).

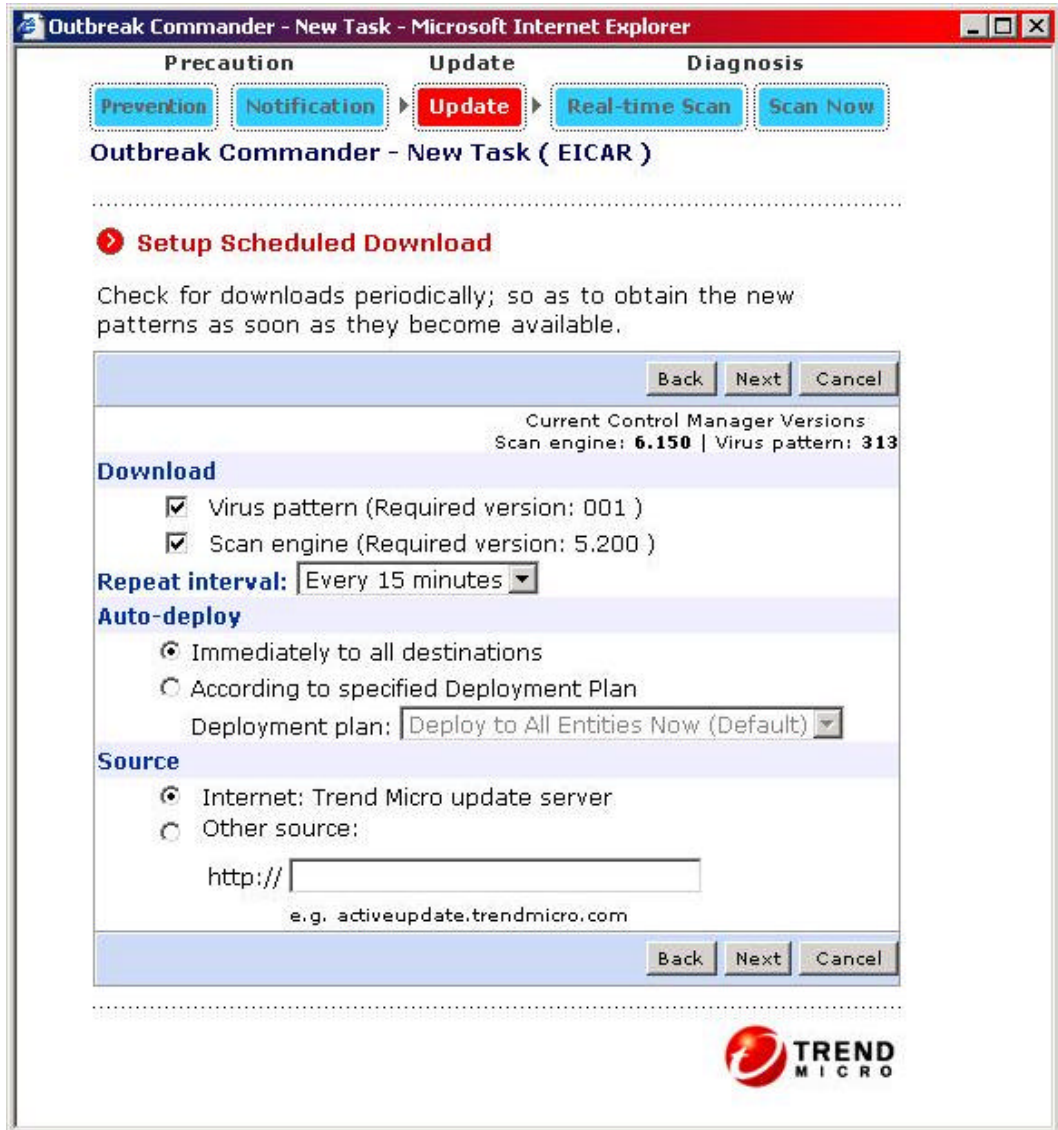
Figure 5.
The Notification stage



UPDATE STAGE

You can determine the download policy for the virus pattern and scan engine. Note that you can view the required and current versions of these components(Figure 6).

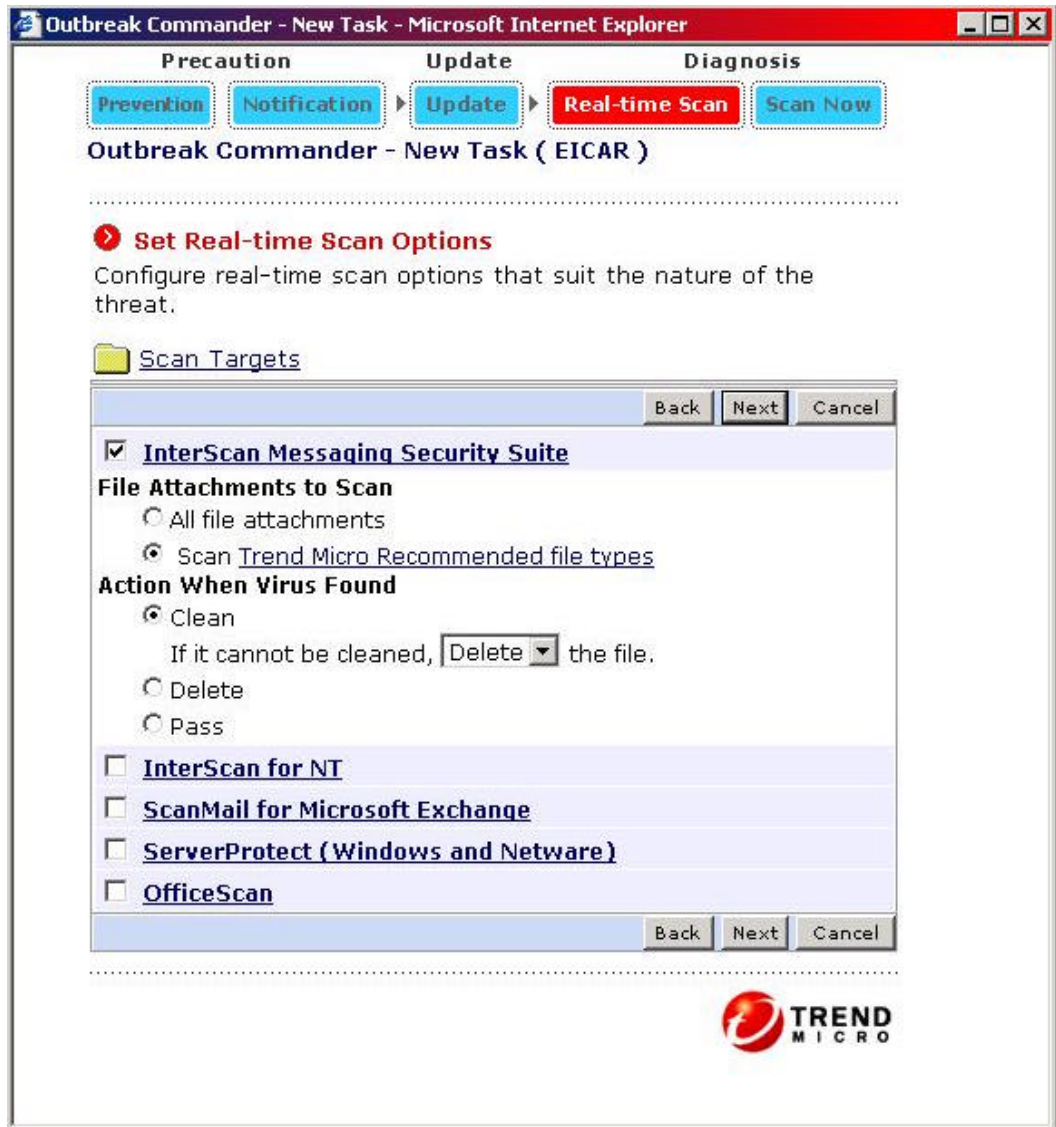
Figure 6.
The upload stage



THE REAL-TIME SCAN STAGE

You can determine the policy once the virus pattern file and scan engine are available (Figure 7).

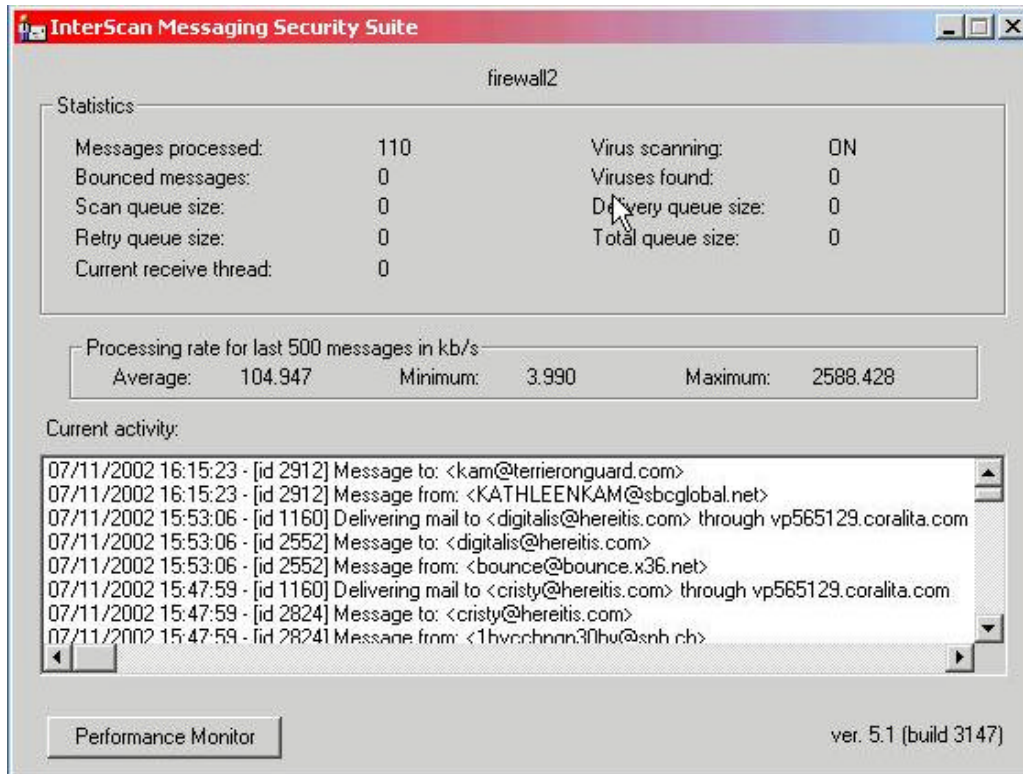
Figure 7.
Real-time scan



THE SCANNOW STAGE

As in Step 7, you can determine the policy once the virus pattern file and scan engine are available.

Figure 8:
Test message



SEND AN INFECTED TEST MESSAGE

Perform the following steps, once the OPS has been initiated for the EICAR virus:

1. Send an email to a test account, with the EICAR antivirus testfile, as an attachment (EICAR.com). Refer to The Prevention Stage.
2. Verify that the test account received the email and that the attachment has been removed.

VERIFY THAT THE TEST IS SUCCESSFUL

In this example, Trend Micro engineers used InterScan Messaging Security Suite. Therefore, we monitored the IMSS Statistics dialog box to check that the email message was received. Note the first entry for 07/11/2002 16:15:23 - [jid 2912] as shown in Figure 8. This entry shows

that a message was sent by KATHLEENKAM@sbcglobal.net to kam@terrieronguard.com

Logs | eManager Logs | Today & 99

Date:	2002/07/11
Time:	16:15:24
Message ID:	1E24B87B-7C41-4F5C-8182-48B67F303972
Sender:	KATHLEENKAM@sbcglobal.net
Recipient:	kam@terrieronguard.com
Subject:	eicar test 11 july 2002 4:16 pm pst
Filter Type:	SPAM FILTER
Filter Settings:	Keyword expression: EICAR.COM
Action on Content:	Not Modified
Action on Message:	Quarantine
Quarantine Area Name:	Default Area

Figure 9.
InterScan Messaging
Security Suite eManager
logs

VIEW AND VERIFY THE LOGS

Figure 9 shows the IMSS eManager content-filtering logs.

Figure 10 shows the Control Manager's Entity Security Logs for IMSS.

Entity | FIREWALL2_IMSS_Agent | Logs | Security Logs | Content Security Violations |
Query | Today & Descending

The first entry, in descending order should be our test example:

#:	1
Received from entity:	07/11/2002 04:15:08 PM
Generated at entity:	07/11/2002 04:15:24 PM
Computer Name:	FIREWALL2
Message ID:	1E24B87B-7C41-4F5C-8182-48B67F303972
Sender:	KATHLEENKAM@sbcglobal.net
Recipient:	kam@terrieronguard.com
Subject:	eicar test 11 july 2002 4:16 pm pst
Filter Name:	SPAM FILTER
Filter Settings:	Keyword expression: EICAR.COM
Action on Content:	Pass
Action on Message:	Quarantine

Figure 10.
Control Manager
Content Security
Violation Log

CONCLUSION

The OPS successfully isolated and quarantined the test email. The test account received the test email with the email attachment removed. The logs from Control Manager and IMSS verify that the Outbreak Prevention Service recognized the EICAR testfile as an attachment. Therefore, the testfile was removed, isolated, and quarantined before it could reach the internal email server, eliminating the possibility of it spreading to other internal users.

In conclusion, the testing procedure described in this document indicates that deploying early policy recommendations with the OPS can help minimize virus outbreaks within your environment. This in turn reduces the associated cleanup costs of virus outbreaks.

August 2002
Trend Micro, Inc.

©2002 by Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of Trend Micro Incorporated. Trend Micro, the t-ball logo, AppletTrap, Control Manager, eManager, GateLock, InterScan, HouseCall, InterScan VirusWall, MacroTrap, NeaTSuite, OfficeScan, PC-cillin, PortalProtect, ScanMail, ScriptClean, ScriptTrap, ServerProtect, SmartScan, TCM, Trend Micro Content Scanning Protocol, Trend Micro Control Manager, Trend Micro CSP, Trend Micro Damage Cleanup Server, Trend Micro Damage Cleanup Services, Trend Micro Outbreak Prevention Services, TrendLabs, Trend VCS, VirusWall, WebManager, WebProtect and WebTrap are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.