

# [NT] TrendMicro Interscan VirusWall Insecurity "Feature"

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0109.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 05/26/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sun, 26 May 2002 18:55:25 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

TrendMicro Interscan VirusWall Insecurity "Feature"

---

## SUMMARY

Trend's Interscan VirusWall has a "feature" in its WinNT/2K implementation that would assist an attacker, spammer, virus sender, in hiding his identity.

## DETAILS

Vulnerable systems:

\* Interscan VirusWall version 3.52 build 1375

In the most installations of Interscan listens on port 25 (SMTP), receives the message, scans it, and then re-sends it to the "real" SMTP daemon (listening on another port), preserving the SMTP-header present in the message.

However, since it does not include the line found with-in the SMTP-header with the sender's real IP, the final message header will not contain the real sender's IP, nor will the program log the real IP of the sender anywhere.

Securiteam: [NT] TrendMicro Interscan VirusWall Insecurity "Feature"

In other words, if you want to track back the origin of a message, you cannot use the message header to discover the sender's IP.

Example:

```
=====
Microsoft Mail Internet Headers Version 2.0
Received: from smtp.domain1.com ([172.0.0.1]) by internal.domain1.com with
Microsoft SMTPSVC(5.0.2195.4905);
Thu, 23 May 2002 20:02:08 -0300
Received: from smtp.domain1.com ([172.0.0.1]) by smtp.domain1.com with
Microsoft SMTPSVC(5.0.2195.2966);
Thu, 23 May 2002 20:02:08 -0300
Subject: Test
=====
```

As you can see in this header, it does not include the IP address of the original message submitter.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[PQuintanilha@abril.com.br](mailto:PQuintanilha@abril.com.br)>  
Pedro Quintanilha.

```
=====
```

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

```
=====
```

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.  
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

---

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Microsoft Active Directory Security Vulnerability (Zero Length)"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)