

## Virus Attack on Al-Masakin Documented

المسكين

This is a typical example of computer virus attacks on Al-Masakin. We find it hard to believe that only one person could be responsible for this. No matter how many times their email is blocked these viruses are systematically mailed to one of our inactive email accounts. Leading us to believe that these types of attacks are generated by a computer robot, or "Bot".

Our other inactive email accounts are systematically spammed with pornography, viruses and insults. Al-Masakin is conducting a detailed investigation into little conspiracies hatched against our media organization.

Cf., <http://www.indybay.org/news/2004/05/1680701.php>

The screenshot shows the Ziplip webmail interface. At the top, there are navigation icons for folders, compose, tools, admin, products, help, and signout. The user's email address, majdur@ziplip.com, is displayed in the top right. On the left, there is a sidebar with folders: Inbox, Sent, SentSecure, Drafts, and Trash. The main area displays a list of emails in the 'Inbox' folder. The list has columns for 'All', 'From', 'Subject', and 'Date'. The emails listed are:

All	From	Subject	Date
<input type="checkbox"/>	leland	1CG5=85	04 Jun 04, 10:38 AM
<input type="checkbox"/>	morris	><>A:>2L5	02 Jun 04, 8:25 PM
<input type="checkbox"/>	hee-sub	1CG5=85	01 Jun 04, 1:35 PM
<input type="checkbox"/>	chakkala	@54;0305< >B4KE 2 "C@F88!	01 Jun 04, 10:16 AM
<input type="checkbox"/>	ramarao	00H0 @5;;0<0 2 ?@5AA5!	01 Jun 04, 12:52 AM
<input type="checkbox"/>	nino	"8?>3@0D80 =0 "030=;5 ?@54;0305B CA;C38 ?>...	31 May 04, 6:41 PM
<input type="checkbox"/>	!;02;8=0 00@8A0	Re:	28 May 04, 10:36 PM
<input type="checkbox"/>	johann	"@0=A?>@B=00 :>AB009=> ?@54;0305...	28 May 04, 3:19 PM
<input type="checkbox"/>	ann-mari	1CG5=85	27 May 04, 8:16 AM

The screenshot shows the header of an email received from leland. The header information is as follows:

**Received:** from cosmo@t-online.de (EHLO pcp461157pcs.shrwd01.ar.comcast.net pcp461157pcs.shrwd01.ar.comcast.net by mail.ziplip.com with ESMTP id IGGKJWL3N0GEKFAHMLNQL4OAKK CJGLJZL3F5GJFT for <>; 04 Jun 2004 07:35:10 -0700 (PDT))

**Date:** Fri, 04 Jun 2004 14:27:30 +0000

**From:** leland <cosmo@t-online.de> [Add | Block]

**To:** majdur@ziplip.com

**Subject:** 1CG5=85

**MIME-Version:** 1.0

**Content-Type:** text/plain; charset=Windows-1251

**Content-Transfer-Encoding:** 8bit

The body of the email contains a block of garbled text, likely a virus payload or spam content:

```
@8H;> ;5B> 8 1=>28;8 A2>N :>;;5:F8N MDD5:B=>3> ?>AB5;L=>3> 15;L.
05 @:85 ?@54AB028B5;8 64CB 00A ?> 04@5AC www.mypresent.ru
```

The screenshot shows the header of an email received from morris. The header information is as follows:

**Received:** from safaa@seznam.cz (EHLO alb-24-194-252-38.nycap.rr.com alb-24-194-252-38.nycap.rr.com [24.194.252.38] by mail.ziplip.com with ESMTP id NZKNHVJYHULSMCP3LZJQOMIBJ3MFGLHWNXAGKPKCK for <>; 02 Jun 2004 17:22:54 -0700 (PDT))

**From:** morris <safaa@seznam.cz> [Add | Block]

**To:** majdur@ziplip.com

**Subject:** ><>A:>2L5

**Date:** Thu, 03 Jun 2004 00:18:14 +0000

**MIME-Version:** 1.0

**Content-Type:** multipart/related; type="multipart/alternative"; boundary="-----\_NextPart\_000\_0000\_88C18E01.34CCFDC2"

**X-Priority:** 3

**X-MSMail-Priority:** Normal

**X-Mailer:** Microsoft Outlook Express 6.00.2600.0000

**X-MimeOLE:** Produced By Microsoft MimeOLE V6.00.2600.0000