



# White Paper

## The Unabomber's Ghost

Aaron Greenspan

Date: February 22, 2006  
Topic Area: Security

It is beginning to look like a new kind of web-based attack has already infected computers across the globe. If this is the case, the epidemic has spread completely under the radar. Without access to the affected servers, it is difficult to be certain exactly what is behind the activity that Think Computer Corporation and many other independent programmers have observed over the past several weeks. However, if this new stealth menace is a virus, as Think's research implies, then at least two worrisome conclusions can be drawn: not a single anti-virus company has bothered to issue a warning (unless the activity described here is the side-effect of a known virus), and the main computer security team commissioned by the United States Department of Defense and currently backed by the Department of Homeland Security has actively ignored a warning about a real global threat that is still spreading as of the writing of this paper.

Dubbed "mail header injection," this relatively new kind of attack takes advantage of an oversight that until recently, almost no one even thought possible, despite more than a decade of

hidden exposure in every web-based form ever created. The idea is that it is possible to force more than one line of text into a text box in an HTML form. Granted, most web browsers do not allow this behavior to take place—pressing the "Enter" key in a text box is typically interpreted as an instruction to submit the active form on a web page—but it is a relatively simple matter to write a program that interacts directly with such a page, bypassing the step of using a web browser completely.

Adding a line to a text box may not seem like a very big deal, but the implications are enormous.

According to research conducted by Think, in the past week, mail header injection attacks have been used to send thousands of spam e-mail messages each *hour*, many of them to users of America Online's popular service. The attacks may be slowing down, or in extreme cases, crashing, some servers, and especially those with access to high bandwidth connections. As few have examined the full scope of the attacks, there are few comprehensive solutions in place. Not one of the band-aid patches available for open-source mail scripts addresses the problem at its source. This is

*There are potentially millions of web sites at risk, and since almost all of them rely on web browsers (that aren't even being used by the attackers) to protect themselves from mail header injection, cleaning up the mess will be a long and arduous task.*





largely because at the present time, it is not clear exactly what that source is. Nonetheless, the patterns created by the problem, which demonstrate that several large companies' servers have been affected, including at least one mail server at Bertelsmann Music Group, indicate a likely virus that affects servers running various versions of the Microsoft Windows operating system.

It has been hypothesized for some time that mail header injection flaws could lay the groundwork for a future virus or worm. The New York PHP users group posted an article on its web site on October 6, 2005, pointing out that "botnets" had been roaming the internet for several months, but at the time the threat did not appear to be spreading. Now, the evidence suggests that we have arrived at that hypothetical future date implied by that article.

The problem involves the deliberate insertion of the Carriage Return and then Line Feed (CRLF) characters into strings of what would otherwise be one-line text, typically contained within HTML TEXT fields in web-based forms. By starting each injected line with keywords such as "Bcc:," "Content-Type:," and "Subject:" that mail routing programs are designed to recognize, attackers can use the appearance of duplicate mail headers to overwrite the original, correct (and usually hard-coded) headers with the new, false ones. Once false headers are in place, inserting hundreds of e-mail addresses into a "Bcc:" header is a trivial matter. The "Content-Type: multipart/alternative;" header can also be used to attach an entirely new message, which can potentially carry an explosive payload, designed to override the intended message. Oddly, some of the massive lists of e-mail addresses that we witnessed in some of the early attacks on Think's server have not manifested themselves in later attacks. This is possibly because the malicious requests

often come in pairs, and so far we have only been able to trigger one notification for each attack, leaving the contents of the other request unknown. In any case, without adequate safeguards, most form handling software will dutifully proceed to deliver the new message to each and every address on the list.

From the attacker's viewpoint, the beauty of this approach is that with a single HTTP request, less than ten kilobytes in size, the victims' servers are forced to do all of the hard work of relaying spam. The attacks are also surprisingly hard to detect; the only obvious indication is an influx of spam, but these days, to the average user, that would hardly appear to be anything new. Customers are usually restricted by their web site hosting companies from using the kinds of diagnostic utilities necessary to analyze log files and detect what is going on, and even those with access to such tools and files rarely use them with enough frequency to be effective at detecting such a clever type of intruder.

We were surprised at just how widespread this problem already appears to be. Since Think's servers were first attacked last week, Think has monitored attacks originating from (in no particular order) Germany, Korea, Italy, Malaysia, Argentina, Kuwait, China, Brazil, Poland, and the United States, among other countries. Think first witnessed the effects of the attacks on February 7, 2006, when it noticed that one of its own web site hosting customers' sites was attracting individuals searching the internet for pornography. This was odd for two reasons: the web site in question belonged to a traditional publishing company, and Think has a policy of not hosting pornographic material.

A program of some sort had evidently replaced all of the site's content, which was controlled by an unprotected content management





system (not one written by Think), with links to pornographic material. Since hundreds of pages had been replaced, all with the exact same text, it looked to be the work of a machine, rather than an individual who would undoubtedly have made a typographical error of one sort or another. What was surprising was that an analysis of the site's logs revealed not one attacker, but more than thirty, all in different locations, who had accessed the site's content management system over a period of twenty days. Pages appeared to have been replaced in a piecemeal fashion at different times by different people, and yet they all ended up with the exact same content.

The same day, Think received an e-mail from one of its web site design partners in Boston, Massachusetts, complaining of people abusing its customers' "Contact Us" forms. The company had already looked into the matter, finding suggestions for how to stop the flow of spam messages on the official web site of PHP, one of several programming languages used to create these types of forms. Though the page on the PHP site specifically devoted to the mail() function explained how to add code to your own program to detect and prevent mail header injection from taking place, we could not find any mention of why the attacks seemed to be increasing in frequency, or taking place at all.

A call to the Computer Emergency Readiness Team (CERT) at Carnegie Mellon University, which works in cooperation with the Department of Homeland Security, revealed that CERT did not know of the problem already. Formally reporting it required the use of the Automated Incident Reporting form at <http://www.cert.org>. Unfortunately, the CERT system erased the detailed report that Think submitted on the first attempt, and by the time the second report was ready to submit a few minutes

later, the log files demonstrating the issue were so large that the CERT system rejected them. Finally, Think wrote up the report a third time and e-mailed it directly to CERT.

Think's log files revealed that the attack on its own server began when one computer requested a series of pages from <http://www.thinkcomputer.com>, as any normal visitor might. However, once the attacker stumbled across the "Contact Us" page, which contains a form, it immediately submitted information to the form four times, and stopped browsing. What happened next was shocking: systems from around the world began submitting data to the same "Contact Us" form, without browsing the rest of the site at all ahead of time. This meant that they had ascertained the URL of the vulnerable form not from the web site, but from some other source, such as a text file, database, or chat room conversation.

Once Think developed its own code to stem the flow of spam and capture data about each attacker, its systems were safe, but a few simple searches revealed that many others were not. Each spam message seemed to contain one of the following similar e-mail addresses in the "Bcc:" field:

- [charieses329@aol.com](mailto:charieses329@aol.com)
- [charleses3229@aol.com](mailto:charleses3229@aol.com)
- [charleses3299@aol.com](mailto:charleses3299@aol.com)

Performing a search for any of these addresses using any popular search engine revealed tens to hundreds of thousands of defaced web sites—evidence of forms intended to update databases, much like our own publishing client's form had been, rather than send out e-mails.

Visiting the hostnames of the attacking systems in a web browser invariably brought up Microsoft Internet Information Server (IIS) error





messages, if any pages appeared at all. This implied that all of the affected, or possibly infected, systems were running Microsoft Windows, though some of the errors made it apparent that different versions of IIS were at risk.

Searching further for information about mail header injection revealed that in the past few weeks, several vendors of Perl, PHP, or other types of e-mail scripts have become aware of the perils of the CRLF character, but none of the security advisories that Think could find mentioned anything about coordinated attacks, or the possibility of a virus. When Think followed up with CERT, its personnel could neither confirm nor deny that they were looking into the problem in any detail. However, CERT did post advisory TA06-045A afterward, which made no mention of the problem.

Think's custom attack detection software has revealed that the attacks on its own servers have been growing in frequency for the past several days, even though its own site is no longer relaying spam messages. Thus, whatever software is causing the attacks to take place does not seem to be aware of the status of a given form that it is attacking.

A few more curious facts remain. The first is the malformed nature of the HTTP POST requests that typically indicate an attack. HTML forms can be submitted by one of two methods: GET or POST, but not both simultaneously. Data in the URL is parsed into GET variables, but POST variables are hidden, and do not appear in the URL. What makes the attacks unusual in this sense is that despite the fact that data is always sent via POST to the vulnerable form, the GET variable "x-up-destcharset" is usually present in the URL string, with the value "106." This variable is completely extraneous, and would not be present in a valid HTTP POST request.

Second, of the multiple servers that Think monitored for this type of attack, several were hit by different computers at the Universiti Teknologi MARA (<http://www.uitm.edu.my>) in Malaysia. This could mean that the UiTM is a source of this malicious software, or simply that an unusual number of the UiTM's servers have been infected.

In addition, it is unusual that the majority of the attacking HTTP requests have arrived without any user agent (or web browser) indicated. However, a few of the most recent attacks have indicated a particular user agent, with the value "Java1.4.2\_03." This might mean that the malicious software is actually a Java applet. It may also be the case that the software actually does not run on Java, and that the user agent signature is being spoofed, perhaps to add a level of confusion to the whole matter.

During the writing of this paper, several more attacks were recorded on Think's server. The computer security and anti-virus communities should launch a more in-depth investigation of mail header injection attacks immediately. It may be the case that this behavior is the result of an already-known virus, or perhaps a flaw in Windows that has already been patched (but not necessarily universally applied). In any case, as you read this, electronic mail bombs are being sent to thousands of web sites, possibly including your own, based on the random sampling of sites we have observed.

There are potentially millions of web sites at risk, and since almost all of them rely on web browsers (that aren't even being used by the attackers) to protect themselves from mail header injection, cleaning up the mess will be a long and arduous task.





## Useful Links

*“Email Header Injection Exploit”*

*[http://www.nyphp.org/phundamentals/  
email\\_header\\_injection.php](http://www.nyphp.org/phundamentals/email_header_injection.php)*

*“PHP: mail”*

*<http://www.php.net/manual/en/function.mail.php>*

## Special Thanks

Special thanks to Andrew Rinaldi of SteadyVision (<http://www.steadyvision.com>), and Marc Garrett, for their assistance investigating this problem.

Copyright © 2006 Think Computer Corporation. All Rights Reserved. Think Computer is a registered trademark of Think Computer Corporation. All other names may be trademarks or registered trademarks of their respective owners.





# Appendix A

February 13, 2006 Apache Log Excerpt - <http://www.thinkcomputer.com>

Scanning attempts are shown here in **blue** for legibility. Attacks are shown in black.

```
200.4.196.122 - - [13/FEB/2006:20:30:52 -0500] "GET /CORPORATE/INDEX.HTML HTTP/1.1" 200 8080 "-" "-"
200.4.196.122 - - [13/FEB/2006:20:30:55 -0500] "GET /CORPORATE/NEWS/PRESSRELEASES.HTML?ID=25 HTTP/1.1" 200 7309 "-" "-"
200.4.196.122 - - [13/FEB/2006:20:30:57 -0500] "GET /CORPORATE/NEWS/RESTASSURED.PDF HTTP/1.1" 200 68934 "-" "-"
200.4.196.122 - - [13/FEB/2006:20:30:59 -0500] "GET /INCREASE/EDUCATION/INDEX.HTML HTTP/1.1" 200 6739 "-" "-"
200.4.196.122 - - [13/FEB/2006:20:31:01 -0500] "GET /SOFTWARE/ALTAMIRA/INDEX.HTML HTTP/1.1" 200 9208 "-" "-"
200.4.196.122 - - [13/FEB/2006:20:31:02 -0500] "GET /SOFTWARE/RENAISSANCE/INDEX.HTML HTTP/1.1" 200 7750 "-" "-"
200.4.196.122 - - [13/FEB/2006:20:31:05 -0500] "GET /INCREASE/SECURITY/INDEX.HTML HTTP/1.1" 200 7307 "-" "-"
200.4.196.122 - - [13/FEB/2006:20:31:06 -0500] "GET /CORPORATE/CONTACTUS.HTML HTTP/1.1" 200 8211 "-" "-"
200.4.196.122 - - [13/FEB/2006:20:31:08 -0500] "POST /CORPORATE/CONTACTUS.HTML HTTP/1.1" 200 8793 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
200.4.196.122 - - [13/FEB/2006:20:31:10 -0500] "POST /CORPORATE/CONTACTUS.HTML HTTP/1.1" 200 6007 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
200.4.196.122 - - [13/FEB/2006:20:31:12 -0500] "POST /CORPORATE/CONTACTUS.HTML HTTP/1.1" 200 6007 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
200.4.196.122 - - [13/FEB/2006:20:31:13 -0500] "POST /CORPORATE/CONTACTUS.HTML HTTP/1.1" 200 6007 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
202-58-85-8.UITM.EDU.MY - - [13/FEB/2006:20:33:24 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-DESTCHARSET=106 HTTP/1.1" 200 6007 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
202-58-85-8.UITM.EDU.MY - - [13/FEB/2006:20:33:25 -0500] "GET /CORPORATE/HISTORY.HTML HTTP/1.1" 200 6167 "-" "-"
202-58-85-8.UITM.EDU.MY - - [13/FEB/2006:20:33:27 -0500] "GET /CORPORATE/NEWS/PRESSRELEASES.HTML?ID=24 HTTP/1.1" 200 8443 "-" "-"
202-58-85-8.UITM.EDU.MY - - [13/FEB/2006:20:33:29 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-DESTCHARSET=106 HTTP/1.1" 200 6007 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
211.219.167.231 - - [13/FEB/2006:21:16:27 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-
```





```
DESTCHARSET=106 HTTP/1.1" 200 5904 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
140.134.4.80 - - [13/FEB/2006:21:24:10 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-
DESTCHARSET=106 HTTP/1.1" 200 4757 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
HOST193-181.POOL82189.INTERBUSINESS.IT - - [13/FEB/2006:21:30:42 -0500] "POST /CORPO-
RATE/CONTACTUS.HTML?X-UP-DESTCHARSET=106 HTTP/1.1" 200 4757 "HTTP://WWW.THINKCOMPUTER.COM/
" "_ "
62.116.40.112 - - [13/FEB/2006:21:37:55 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-
DESTCHARSET=106 HTTP/1.1" 200 4757 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
BXP238.INTERNETDSL.TPNET.PL - - [13/FEB/2006:22:31:03 -0500] "POST /CORPORATE/
CONTACTUS.HTML?X-UP-DESTCHARSET=106 HTTP/1.1" 200 4757 "HTTP://WWW.THINKCOMPUTER.COM/"
"_"
BXP238.INTERNETDSL.TPNET.PL - - [13/FEB/2006:22:31:25 -0500] "POST /CORPORATE/
CONTACTUS.HTML?X-UP-DESTCHARSET=106 HTTP/1.1" 200 4757 "HTTP://WWW.THINKCOMPUTER.COM/"
"_"
219.93.95.25 - - [13/FEB/2006:22:47:38 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-
DESTCHARSET=106 HTTP/1.0" 200 4737 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
220-135-190-237.HINET-IP.HINET.NET - - [13/FEB/2006:22:48:18 -0500] "POST /CORPORATE/
CONTACTUS.HTML?X-UP-DESTCHARSET=106 HTTP/1.1" 200 4757 "HTTP://WWW.THINKCOMPUTER.COM/"
"_"
219.252.192.211 - - [13/FEB/2006:23:04:15 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-
DESTCHARSET=106 HTTP/1.1" 200 4757 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
212.161.126.193 - - [13/FEB/2006:23:21:15 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-
DESTCHARSET=106 HTTP/1.1" 200 4757 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
212.161.126.193 - - [13/FEB/2006:23:21:21 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-
DESTCHARSET=106 HTTP/1.1" 200 4757 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
199.219.184.51 - - [13/FEB/2006:23:39:13 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-
DESTCHARSET=106 HTTP/1.0" 200 4737 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
65.99.198.36 - - [13/FEB/2006:23:40:13 -0500] "POST /CORPORATE/CONTACTUS.HTML?X-UP-
DESTCHARSET=106 HTTP/1.1" 200 4757 "HTTP://WWW.THINKCOMPUTER.COM/" "-"
CABLE-63-135-24-231.SUDBURY.DYN.PERSONAINC.NET - - [13/FEB/2006:23:59:29 -0500] "POST /
CORPORATE/CONTACTUS.HTML?X-UP-DESTCHARSET=106 HTTP/1.0" 200 4737 "HTTP://
WWW.THINKCOMPUTER.COM/" "-"
```





# Appendix B

*Select Mail Injection Notifications (produced by Think attack detection software)*

MAIL INJECTION NOTIFICATION  
-----

ATTACKER: 210.183.221.125 (210.183.221.125)  
VICTIM: WWW.THINKCOMPUTER.COM  
REFERRING PAGE: HTTP://WWW.THINKCOMPUTER.COM/  
USER AGENT SIGNATURE:  
HTTP REQUEST METHOD: POST  
HTTP REQUEST URI: /CORPORATE/CONTACTUS.HTML?X-UP-DESTCHARSET=106

[No HTTP User Agent Found.]

\$\_POST AFFECTED FIELDS: FIRSTNAME  
\$\_POST CONTENTS:

---

ARRAY

(  
    [RATING] => SAID1688@THINKCOMPUTER.COM  
    [FIRSTNAME] => IS  
CONTENT-TYPE: MULTIPART/ALTERNATIVE; BOUNDARY=953717D5DFC7868D43C1FB6A65F545CE  
MIME-VERSION: 1.0  
SUBJECT: AM CLEARING OUT THE COURT T COSTS  
BCC: CHARLESSES3299@AOL.COM

THIS IS A MULTI-PART MESSAGE IN MIME FORMAT.

--953717D5DFC7868D43C1FB6A65F545CE  
CONTENT-TYPE: TEXT/PLAIN; CHARSET="US-ASCII"  
MIME-VERSION: 1.0  
CONTENT-TRANSFER-ENCODING: 7BIT

OFFICERS OF POLICE, TOGETHER WITH SOME OF THE GUARD, CONDUCTED OUT THE CONDEMNED, WHO WAS PLACED IN THE PILLORY. HIS WAS A SORT OF WOODEN YOKE LAID ACROSS THE SHOULDERS OF THE DELINQUENT

--953717D5DFC7868D43C1FB6A65F545CE--

.

[INFORMATION] => SAID1688@THINKCOMPUTER.COM  
[LASTNAME] => SAID1688@THINKCOMPUTER.COM  
[COMMENTS] => SAID1688@THINKCOMPUTER.COM  
[PHONE] => SAID1688@THINKCOMPUTER.COM  
[SUBMIT] => SAID1688@THINKCOMPUTER.COM  
[ORGANIZATION] => SAID1688@THINKCOMPUTER.COM  
[EMAIL] => SAID1688@THINKCOMPUTER.COM  
[IMPROVE] => SAID1688@THINKCOMPUTER.COM  
)

---





MAIL INJECTION NOTIFICATION  
-----

ATTACKER: 65.208.122.46 (65.208.122.46)  
VICTIM: WWW.THINKCOMPUTER.COM  
REFERRING PAGE: HTTP://WWW.THINKCOMPUTER.COM/  
USER AGENT SIGNATURE: JAVA1.4.2\_03  
HTTP REQUEST METHOD: POST  
HTTP REQUEST URI: /CORPORATE/CONTACTUS.HTML?X-UP-DESTCHARSET=106

\$\_POST AFFECTED FIELDS: FIRSTNAME  
\$\_POST CONTENTS:

---

ARRAY

(  
    [RATING] => THAT2906@THINKCOMPUTER.COM  
    [FIRSTNAME] => DAMN  
CONTENT-TYPE: MULTIPART/ALTERNATIVE; BOUNDARY=CC3BCA75A493C1369C4EA5D41EA10275  
MIME-VERSION: 1.0  
SUBJECT: OF DRESS TO COVER HIMSELF  
BCC: CHARLESES3229@AOL.COM

THIS IS A MULTI-PART MESSAGE IN MIME FORMAT.

--CC3BCA75A493C1369C4EA5D41EA10275  
CONTENT-TYPE: TEXT/PLAIN; CHARSET="US-ASCII"  
MIME-VERSION: 1.0  
CONTENT-TRANSFER-ENCODING: 7BIT

H PRISIDINT HARDLY MISSED HIM BE MORE THIN A FOOT AT TH GATE, BUT TH ONGRESSMAN BEIN  
FORMERLY WAN IV OSBY S  
--CC3BCA75A493C1369C4EA5D41EA10275--

.

[INFORMATION] => THAT2906@THINKCOMPUTER.COM  
[LASTNAME] => THAT2906@THINKCOMPUTER.COM  
[COMMENTS] => THAT2906@THINKCOMPUTER.COM  
[PHONE] => THAT2906@THINKCOMPUTER.COM  
[SUBMIT] => THAT2906@THINKCOMPUTER.COM  
[ORGANIZATION] => THAT2906@THINKCOMPUTER.COM  
[EMAIL] => THAT2906@THINKCOMPUTER.COM  
[IMPROVE] => THAT2906@THINKCOMPUTER.COM  
)

---

MAIL INJECTION NOTIFICATION





-----  
ATTACKER: MAIL1.BMGSMUSIC.COM (170.171.250.51)  
VICTIM: WWW.THINKCOMPUTER.COM  
REFERRING PAGE: HTTP://WWW.THINKCOMPUTER.COM/  
USER AGENT SIGNATURE:  
HTTP REQUEST METHOD: POST  
HTTP REQUEST URI: /CORPORATE/CONTACTUS.HTML?X-UP-DESTCHARSET=106

[No HTTP User Agent Found.]

\$\_POST AFFECTED FIELDS: FIRSTNAME  
\$\_POST CONTENTS:

---

ARRAY

(  
    [RATING] => HIM7769@THINKCOMPUTER.COM  
    [FIRSTNAME] => HE  
CONTENT-TYPE: MULTIPART/ALTERNATIVE; BOUNDARY=575654BD51285D33072CEAF2FE5B62BE  
MIME-VERSION: 1.0  
SUBJECT: TH LANNIGANS BOUGHT A PIANNY  
BCC: STARLAK8099@AOL.COM

THIS IS A MULTI-PART MESSAGE IN MIME FORMAT.

--575654BD51285D33072CEAF2FE5B62BE  
CONTENT-TYPE: TEXT/PLAIN; CHARSET="US-ASCII"  
MIME-VERSION: 1.0  
CONTENT-TRANSFER-ENCODING: 7BIT

TTO TO OBSERVE BOTH HER AND OUISE SO CLOSELY, AND EVEN AGAINST HIS OWN WILL TO  
--575654BD51285D33072CEAF2FE5B62BE--

.

[INFORMATION] => HIM7769@THINKCOMPUTER.COM  
[LASTNAME] => HIM7769@THINKCOMPUTER.COM  
[COMMENTS] => HIM7769@THINKCOMPUTER.COM  
[PHONE] => HIM7769@THINKCOMPUTER.COM  
[SUBMIT] => HIM7769@THINKCOMPUTER.COM  
[ORGANIZATION] => HIM7769@THINKCOMPUTER.COM  
[EMAIL] => HIM7769@THINKCOMPUTER.COM  
[IMPROVE] => HIM7769@THINKCOMPUTER.COM  
)

---

MAIL INJECTION NOTIFICATION





-----  
ATTACKER: EXCHANGE1.CGI-MAIN.CGIPHARMA.COM (64.148.46.1)  
VICTIM: WWW.THINKCOMPUTER.COM  
REFERRING PAGE: HTTP://WWW.THINKCOMPUTER.COM/  
USER AGENT SIGNATURE:  
HTTP REQUEST METHOD: POST  
HTTP REQUEST URI: /CORPORATE/CONTACTUS.HTML?X-UP-DESTCHARSET=106

[No HTTP User Agent Found.]

\$\_POST AFFECTED FIELDS: FIRSTNAME  
\$\_POST CONTENTS:

---

ARRAY

(  
    [RATING] => TRUTH8766@THINKCOMPUTER.COM  
    [FIRSTNAME] => TIMES  
CONTENT-TYPE: MULTIPART/ALTERNATIVE; BOUNDARY=E90F46D05B9EC3EE5BB3E84EF4EDFC63  
MIME-VERSION: 1.0  
SUBJECT: AND HER FRIGHTENED DAUGHTERS, THEY ROWED INTO  
BCC: WINT0LYMPL0VR99@AOL.COM

THIS IS A MULTI-PART MESSAGE IN MIME FORMAT.

--E90F46D05B9EC3EE5BB3E84EF4EDFC63  
CONTENT-TYPE: TEXT/PLAIN; CHARSET="US-ASCII"  
MIME-VERSION: 1.0  
CONTENT-TRANSFER-ENCODING: 7BIT

BE WANDHERIN OVER TH FACE IV TH WURRULD BUT M NOT PROUD IV ME LOOKS AN WILL REMARK  
THAT IDDY OSENFELT WAS CAPABLY DIRECTED BE TH IDITORS IV NGLAND, THIM HEARTS IV OAK,  
THAT TH MERICAN NAVY WAS ADVISED BE OUR MOS INARGETIC CORRYSPONDINTS  
--E90F46D05B9EC3EE5BB3E84EF4EDFC63--

.

[INFORMATION] => TRUTH8766@THINKCOMPUTER.COM  
[LASTNAME] => TRUTH8766@THINKCOMPUTER.COM  
[COMMENTS] => TRUTH8766@THINKCOMPUTER.COM  
[PHONE] => TRUTH8766@THINKCOMPUTER.COM  
[SUBMIT] => TRUTH8766@THINKCOMPUTER.COM  
[ORGANIZATION] => TRUTH8766@THINKCOMPUTER.COM  
[EMAIL] => TRUTH8766@THINKCOMPUTER.COM  
[IMPROVE] => TRUTH8766@THINKCOMPUTER.COM  
)

---

