

## Re: strange SMTP traffic from Korea

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-11/0324.html>

---

**From:** jayjwa (jayjwa\_at\_hotspam.microsoftsuk)

**Date:** 11/30/03

Date: Sat, 29 Nov 2003 23:37:54 -0500

Damian Menscher wrote:

> *I tried posting this to the incidents list a few weeks ago, but the*  
> *moderator didn't find it worthy. Our local security people don't*  
> *speak Korean, so they say there's nothing they can do. So, I'm*  
> *asking for help here:*

>

> *Since Oct 13 we've been seeing some rather unusual traffic from*  
> *various IPs in Korea (list below). It was leaving logs like the*  
> *following:*

Funny you mention this... What's up with that country? I banned Korea along time ago from my MTA, but they are always trying to connect to someplace to try something. I just had one about 20 min. ago. I had him mapped out before he disconnect- a Windoze machine with a ton of services on it, including a sql server set to its default install. I hide behind a proxy and then checked out it's http, and it was of course all in Korean, but I made out somekinda login, one on the left, and one on the right. They were running Apache 1x, but this wasn't basic auth, it was something they cooked up themselves. I've never seen a more insecure computer before, so that got me to thinking, maybe all this crap we see from them is really due to compromised systems? e.g., they get owned hard then Oh, Look! now it appears that Korea is playing monkey tag with your mail server...

The authorities don't speak the language, so they ain't gonna do anything? Great, then I hope they are just as dumb-founded going the otherway too, does this mean I get to brute-force that login screen, because maybe the authorities don't speak the language? Bhaaa...

t=Atr2-WBS-----Mod\_SSL/GPG/OpenSSL-----

[jayjwa] Was I helpful? <https://atr2.ath.cx/affero.php>

<rot13>

Znvy: wnlwjn@nge2.ngu.pk

Raq glenaal: Nffnfvangr Ovyv Tngrf

Jvaqbjf vf n qvfrnfr

</rot13>

??? <https://atr2.ath.cx/who-we-are.html>

-----Linux Tough.Powered By Slackware-----HTTPS/FTP-----RLF#37=