Script - Move Infected Emails to Quarantine and Notify Users

The following script will do the following:

1. Parse email headers from ClamScan Results
2. Move infected email to `$QUARANTINE` folder
3. Construct email messages
4. Email the users who has any infected emails in their mailbox

```
#! /bin/bash

ADMIN="admin@domain.com" # Admin email
QUARANTINE="/quarantine/directory/" # Quarantine folder with trailing slash
HEADER="The emails listed has been moved to quarantine and will be deleted after 30 days. If you have any concerns, please contact the server administrator"
FOOTER="This is an automated email through ClamScan results, please find the script details at 'https://wiki.twcloud.tech/books/linux/page/script---move-infected-emails-to-quarantine-and-notify-users'"

# Getting email information
[ -z "$1" ] && echo "File parameter missing" && exit 1
[ ! -f "$1" ] && echo "File not found / not a regular file" && exit 1
declare -A emails
while read i; do
    file=`echo "$i" | sed -e 's/\: \ .*FOUND//'`
    if [ ! -f "$file" ]; then
        continue
    fi
    infection=`echo "$i" | sed -n 's/\: \ .*FOUND//'`
    to=`cat "$file" | grep -m 1 "^Envelope-to\: \s\+" | sed 's/Envelope-to\: \ //' | grep -EiEio '\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b'`
    # Try find To: header if Envelope-to: not found
```

```
    [[ -z "$to" ]] && to=`cat "$file" | grep -m 1 "^To\:\s\+" | sed 's/To\:\ //' | grep -EiEio
'\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b'`
    from=`cat "$file" | grep -m 1 "^From\:\s\+" | sed 's/From\:\ //'`
    d=`cat "$file" | grep -m 1 "^Delivery-date\:\s\+" | sed 's/Delivery-date\:\ //'`
    subject=`cat "$file" | grep -m 1 "^Subject\:\s\+" | sed 's/Subject\:\ //'`

    # Send empty "$to" to admin
    [[ -z "$to" ]] && to="$ADMIN"

    # Construct email message
    [[ -z "${emails[$to]}" ]] && emails[$to]="$HEADER"
    emails[$to]="${emails[$to]}\n\nFrom: $from\nDate: $d\nSubject: $subject"

    # Move emails to quarantine
    mv "$file" "$QUARANTINE"
done < "$1"

# Notify email users that the emails are sent to quarantine
for k in "${!emails[@]}"; do
    echo -e "${emails[$k]}\n----------\n$FOOTER" | mail -s "Infected emails quarantined" -c
"$ADMIN" $k
done
```

Revision #5
Created 18 June 2017 23:24:47 by Tingwai
Updated 18 June 2017 23:50:24 by Tingwai