Server di posta con email criptate per garantire la confidenzialità

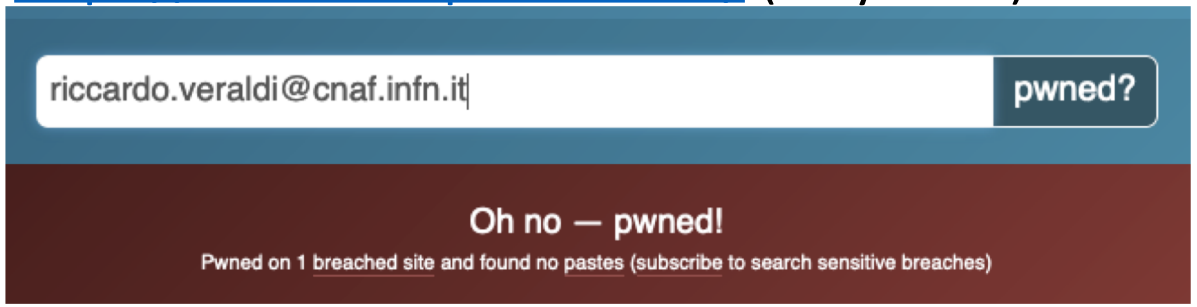
Riccardo Veraldi

Data Breach

- un incidente di sicurezza informatica in cui dati sensibili, protetti o riservati sono stati potenzialmente visualizzati, violati e utilizzati da un individuo non autorizzato a farlo

Email and password data breach

- Jan 2019: Massive Data Breach Exposes 773 Million Emails, 21 Million Passwords
- https://haveibeenpwned.com/ (Troy Hunt)



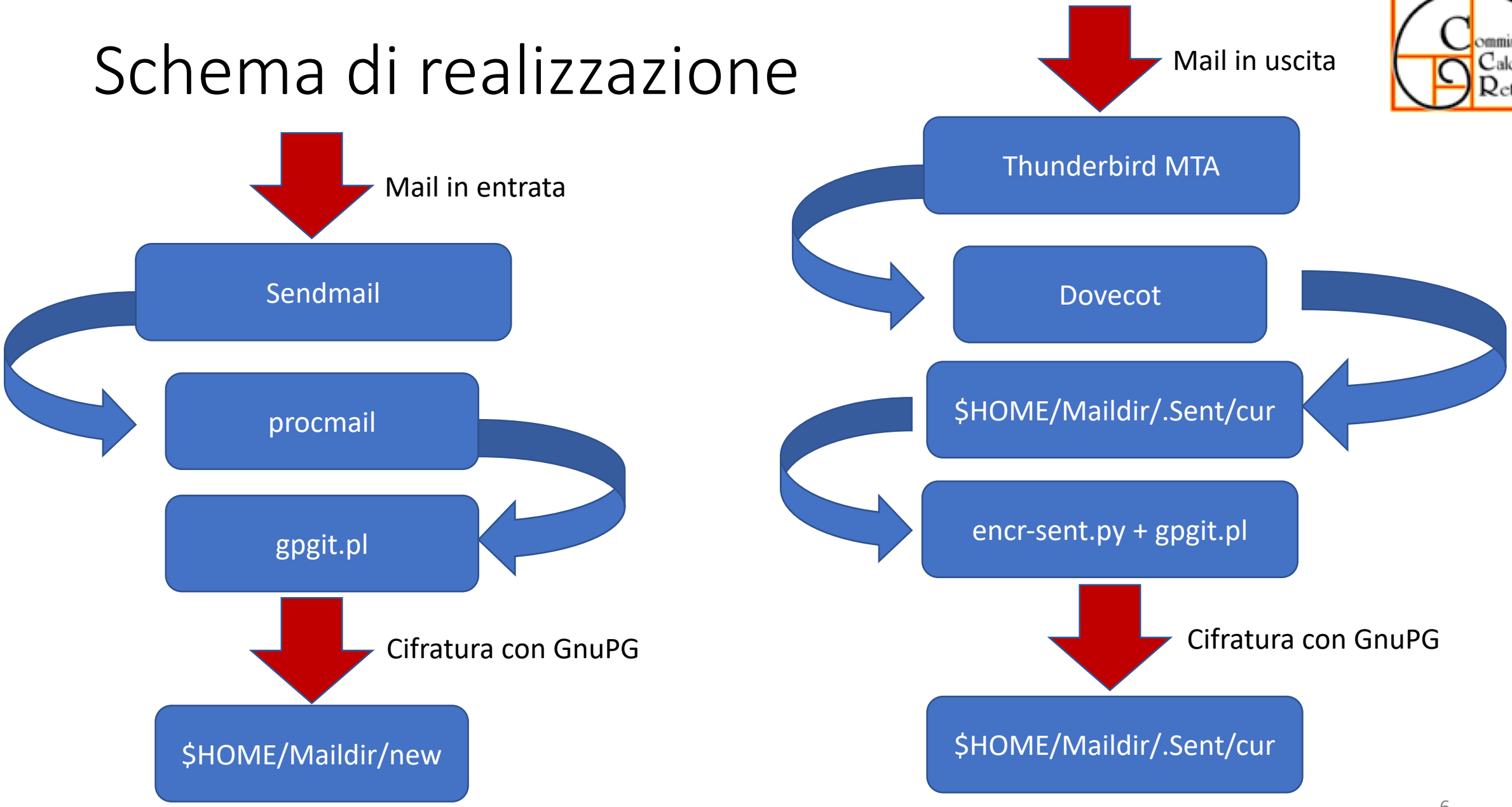
- In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moɈuƎq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

In buona compagnia…

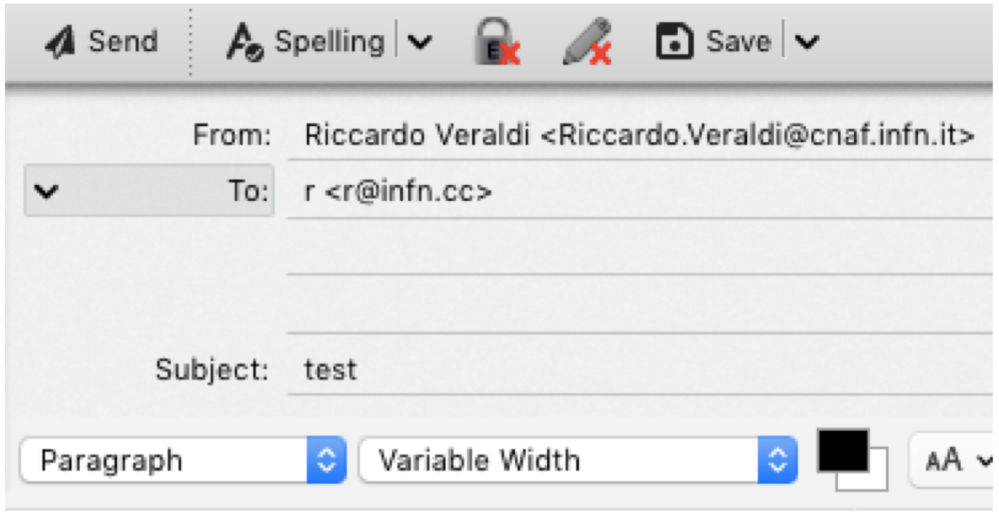
Email encryption

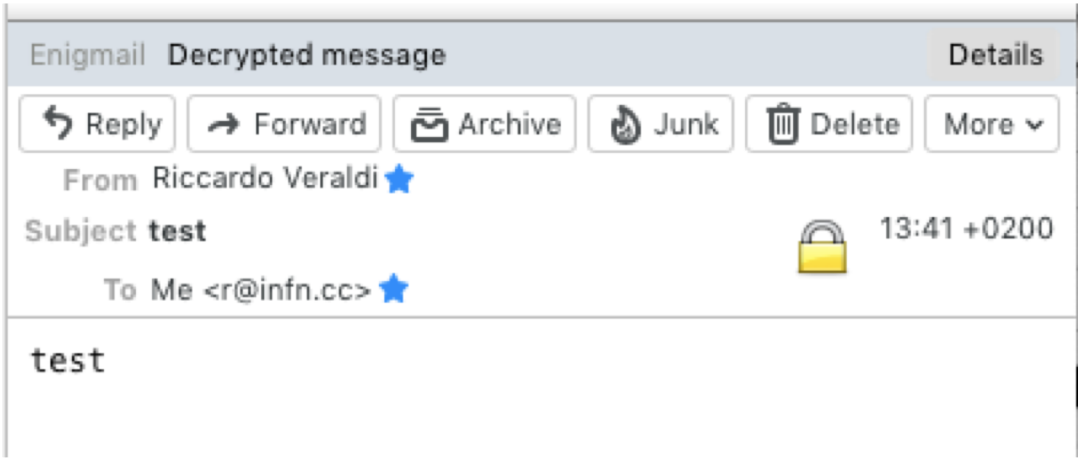
- Perchè non criptare TUTTI i messaggi di posta in entrata ?
  - Ogni messaggio viene cifrato su disco e solo il destinatario può decifrarlo
- Modalità classica
  - End-to-End email encryption
    - S/MIME
    - PGP (OpenPGP)
    - GnuPG (OpenPGP)
    - Bitmessage (con IMAP/POP bridges)
  - Il mittente deve avere la chiave pubblica del destinatario con cui cifra e/o firma il messaggio inviato
    - In caso di S/MIME i certificati X509 hanno spesso validità limitata nel tempo
- Modalità alternativa
  - tutte le mail che ricevo vengono cifrate sul mail server (IMAP) indipendentemente dal fatto che il mittente utilizzi una particolare tecnologia di encryption per inviare un messaggio

Schema di realizzazione



Esempio ricezione di un messaggio






```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.22 (GNU/Linux)

hQIMA/DF8Eo+NCExAQ/9Howo/O9LEpYmBea7YVnb/4efIp7IO8orGhy4C3dMny9d
TSkzKZu2mgqDJhQGbPeqS3C64MyHLDQqaQP9IBp96Ur52a/F+sfyEGPJ3/J+FNCZ
8pFFRVr8BeeVJ/Ls8Y5wLlrRKoNeZQF5DDy2bJEY1io1A+T+Iy+hHRWakVHAAMUl
n23XEQGh8qaNfGHOIFCKknkrYrjfzAEyDichYpRN/duYTouX4jE1BkutP+auZyNO
QyOs6zpRrAKGKRh2TxNOHVj/aqcxJfJd3fTE8Ucpmqf1iD2shUF923Qc79Xsq4IE
8gYorMivucEVu8VeE4NAhR6grzE8CreHmNkVvFe2m/kSfuo+jp1xZORh4NDz3aVP
uPJmOGWhv2pxMQu8u1XqJ91esMilHGmvYH40wJhmZ5iPi9k4TzzoJ/jUqs+ytitR
bEU6088XnT6RmOkR+nhTLUAI5enL9Cu2Yh7rJyBAAlb6PD1/lt0V7E9pPqdon/SO
8sf0fJbloXzJglA7n/xEn/WiRAJ4j3MQHFy6wiXyOywzosjh1FYCdfBnvU9ZyAYk
Rf24/s52sYkF4jUShZFhLwe13ES9/dUP7QS9STl/apO0fcBs2g983IQFgW4IaShO
eT5macKZYRGwOgc89vZsA7PlUjtR2sGIEM674MjIh58eX8XwKRva8HUritT5UVvS
kwGxFwPWX1Fk9Tw5ng2m1XzDEDE3YjPHHQC6p9yfDNz7Zaqv/jl+w2ZuorXArN82
x5FRRsGkkthMnyPbxsMv7B4peQDo2//ue/AQp/b4kCilH9FFnh7j9CjGMiApiR/K
WoFel6MK8M65RZoZ5GQhKGKDmIzXuUL0aamrQ2Bd3+EGBNg5LXUB0FNz1KCoRRXd
7sSKPA==
=TFO9
-----END PGP MESSAGE-----
```

Componenti lato server

- Sendmail configurato per utiizzare «procmail»
- .procmailrc

```
DEFAULT="$HOME/Maildir/"
MAILDIR="$HOME/Maildir/"
:0 f
| /usr/local/bin/gpgit.pl r@infn.cc
```

- gpgit.pl (https://gitlab.com/mikecardwell/gpgit)
- Chiave pubblica GPG per ogni utente nella propria $HOME/.gnupg
- Dovecot
- *Opzionale* encr-sent.py (https://github.com/rveraldi/encr-sent)
  - Per cifrare automaticamente le mail nel folder Sent

Componenti lato MUA

- Client di posta che possa gestire la cifratura con chiavi GPG in modo da potere Decriptare i messaggi di posta con la chiave GPG privata dell'utente
  - Thunderbird + Enigmail (Windows, Linux, MacOS X) TESTED
  - Outlook + GPG4Win (Windows)
  - Apple Mail + GPGTools (MacOS X)
  - Canary Mail (MacOS X)
  - Mutt (Linux, MacOS X)
  - Mailvelope (Web Browser plugin)

Mail in uscita cifratura (IMAP Sent folder)

- Non vengono direttamente cifrate dal server (non passano per procmail)
- Soluzioni
  - Utilizzare Exim come mail server e utilizzare un filtro per i messaggi in uscita
    - Richiede però accesso a un repository locale delle password imap degli utenti
  - Thunderbird setup
    - Disabilitare la copia dei mail in uscita nel folder Sent
    - Abilitare Auto Bcc to self
    - Abilitare un filtro (se il messaggeio e' per me stesso copia in Sent)
  - encr-sent.py
    - Daemon che monitora in modo efficiente tramite inotify (Linux kernel subsystem) la cartella Sent dell'utente sul server IMAP (Dovecot) e cifra i messaggi quando vengono scritti nella cartella
  - Non copiare le mail in uscita sul server IMAP

Applicazioni

- Server di posta per sedi/servizi con particolari esigenze di privacy
  - INFN-CERT
  - Presidenza INFN (?)
  - Altri ?