ETH zürich

ETH Zürich Mail Filtering Service

NetSec 2020

Some Statistics

- In 2019, our filter blocked 287 million messages (80% of inbound mail)
- Since 2003, our filters have blocked 3 billion messages

```
TCP/IP Connection from 131.111.8.59                                  connect
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
EHLO spamcentral.net                                                 helo
   250 phil1.ethz.ch Hello spamcentral.net  [131.111.8.59]
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
MAIL FROM: spammer@spamcentral.net  SIZE=381                         recipient
   250 OK
RCPT TO: tom@ethz.ch
  250 Accepted
RCPT TO: dick@ethz.ch
  250 Accepted
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DATA                                                                 data
  354 Enter message, ending with "." on a line by itself
Subject:      A Hot deal!
From:         admin@ethz.ch
Date:         08/30/2007 16:00
To:           santaclaus@northpole.net
Received:   from mail1.pole.net [83.4.6.232]

The PRGN stock price is about to soar!
Buy it now to get in on the HOT DEAL!
.
   250 OK id=1GmuOH-0002UW-4R
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
QUIT                                                                 closing
  221 phil1.ethz.ch closing connection
```

TCP/IP Connection from 131.111.8.59 — connect

EHLO spamcentral.net — helo

250 phil1.ethz.ch Hello spamcentral.net [131.111.8.59]

MAIL FROM: spammer@spamcentral.net SIZE=381 — recipient

250 OK

RCPT TO: tom@ethz.ch

250 Accepted

RCPT TO: dick@ethz.ch

250 Accepted

DATA — data

354 Enter message, ending with "." on a line by itself

Subject: A Hot deal!

From: admin@ethz.ch

Date: 08/30/2007 16:00

To: santaclaus@northpole.net

Received: from mail1.pole.net [83.4.6.232]

The PRGN stock price is about to soar!

Buy it now to get in on the HOT DEAL!

.

250 OK id=1GmuOH-0002UW-4R

QUIT — closing

221 phil1.ethz.ch closing connection

TCP/IP Connection from 131.111.8.59 — connect

EHLO spamcentral.net — helo

250 phil1.ethz.ch Hello spamcentral.net [131.111.8.59]

MAIL FROM: spammer@spamcentral.net SIZE=381 — recipient

250 OK

RCPT TO: tom@ethz.ch

250 Accepted

RCPT TO: dick@ethz.ch

250 Accepted

DATA — data

354 Enter message, ending with "." on a line by itself

Subject: A Hot deal!
From: admin@ethz.ch
Date: 08/30/2007 16:00
To: santaclaus@northpole.net
Received: from mail1.pole.net [83.4.6.232]

The PRGN stock price is about to soar!
Buy it now to get in on the HOT DEAL!
.

250 OK id=1GmuOH-0002UW-4R

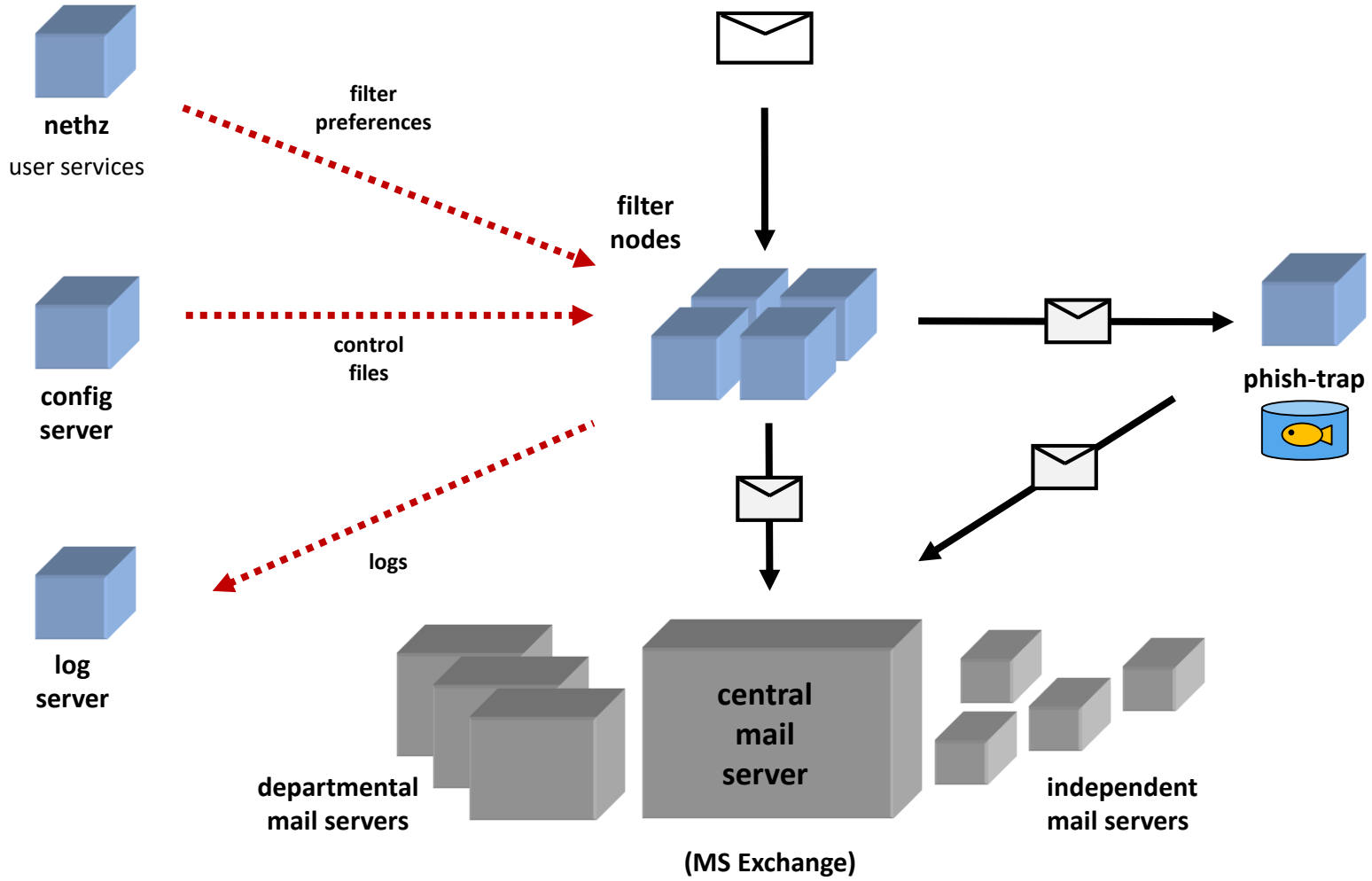
QUIT — closing

221 phil1.ethz.ch closing connection

Mail filter design considerations

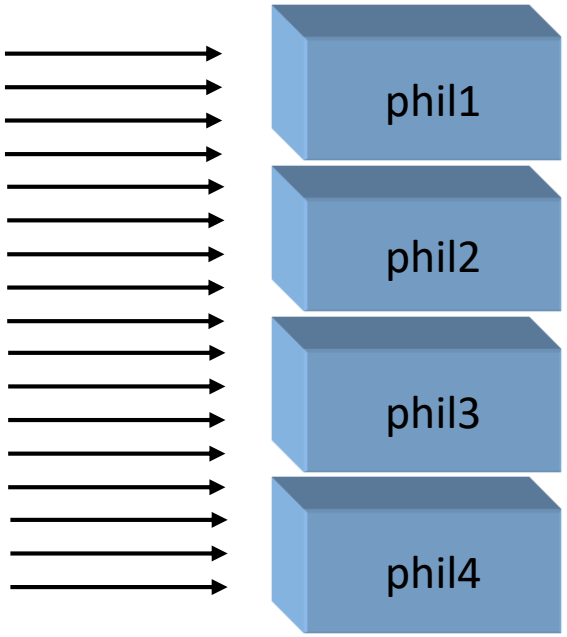
- Will you accept all messages & then filter them
  or reject some messages in the STMP session?
- Will you use a single SMTP session to receive messages
  or use multiple parallel SMTP sessions?
- Will you filter only inbound mail or also filter outbound mail?
- Should the filter have its own DNS server?
- How will you check valid recipient addresses?
  (local list, query a remote database, ask your mail server)
- Will users have individual black & white lists?
- Will users have individual filtering preferences?
  (quarantine, tag, delete)

Filter Architecture (first-generation filter)



Parallel SMTP Sessions (first-generation filter)

100 incoming SMTP sessions per host.



DNS MX records direct a domain's mail to the filter nodes

example:

```
biol.ethz.ch  mx 5  phil1.ethz.ch
biol.ethz.ch  mx 5  phil2.ethz.ch
biol.ethz.ch  mx 5  phil3.ethz.ch
biol.ethz.ch  mx 5  phil4.ethz.ch
```

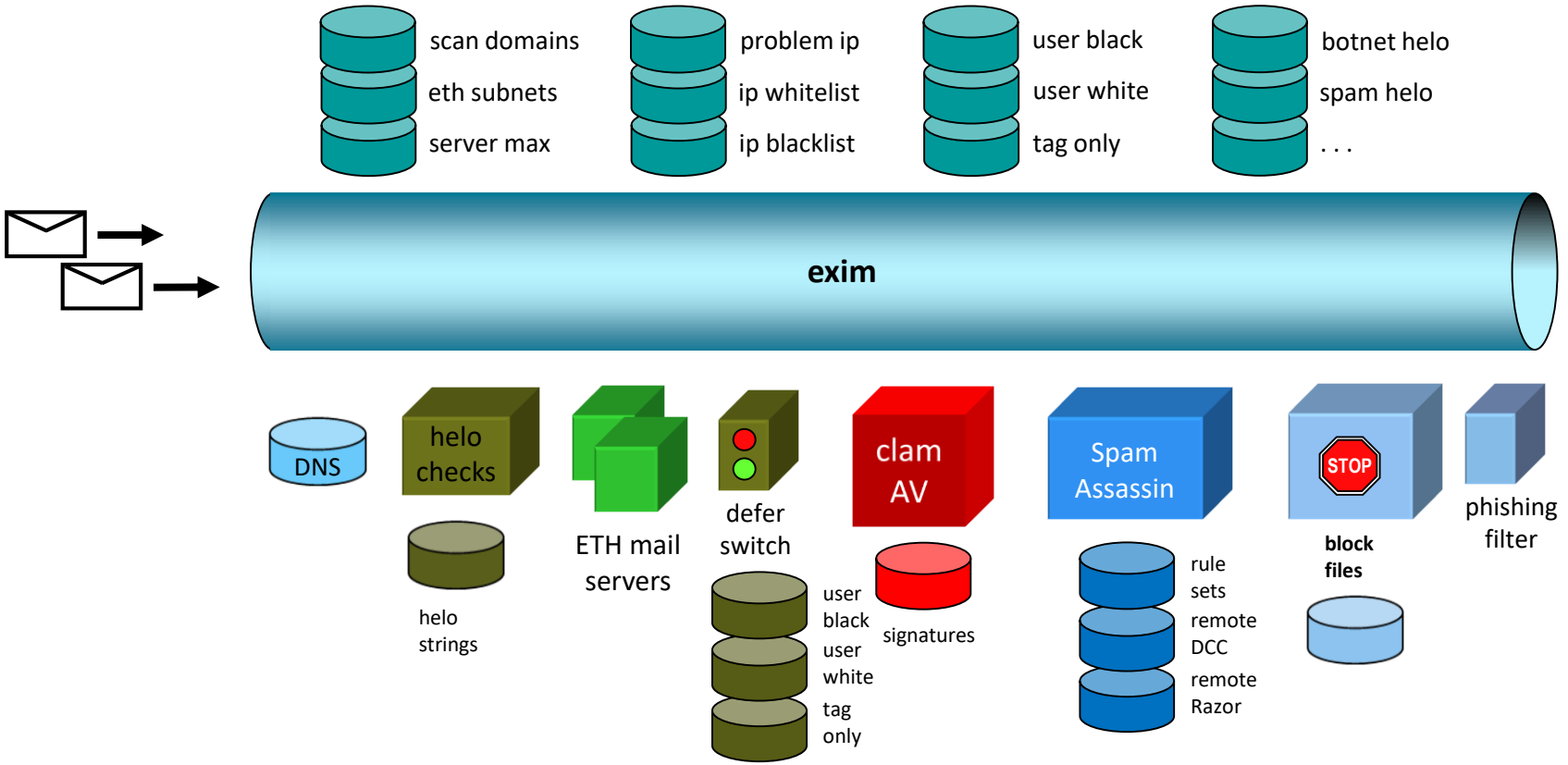
SMTP-time message filtering:

- filtering is done while the SMTP connection is still open
- filtering requires several seconds
- unwanted messages are rejected in the SMTP session, or accepted & tagged
- some recipients in a multi-recipient message may be deferred

Filtering techniques (first-generation filter)

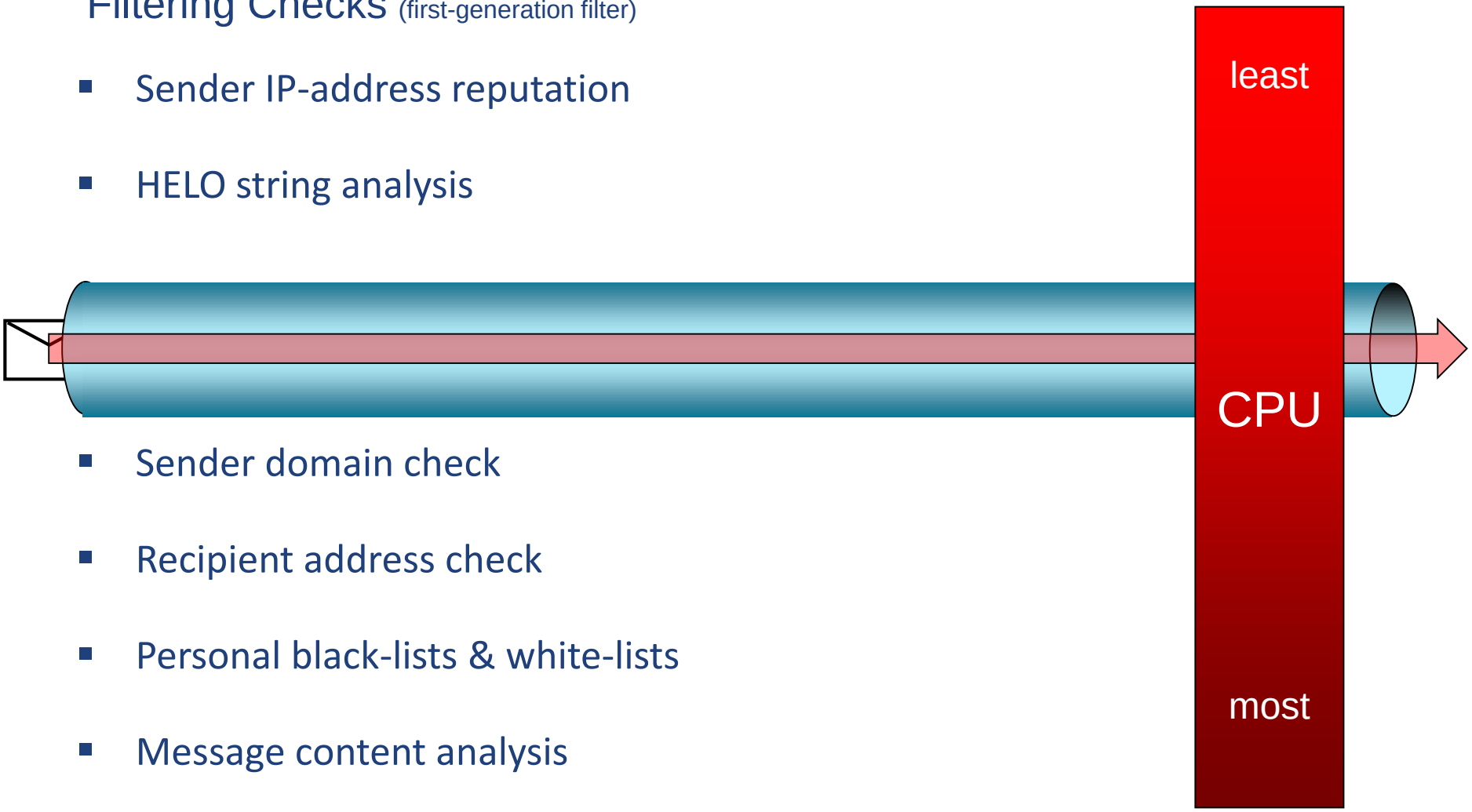
▪ DNS domain queries	detect non-existent sender domains
▪ DNS DOB queries	detect newly-registered sender domains
▪ DNS SPF & DKIM queries	detect forged sender addresses
▪ DNS blacklists	block spam hosts & botnets
▪ DNS blacklists with a high refresh rates	block spam host IP changes
▪ SMTP-time recipient address verification	block “joe jobs”
▪ SMTP HELO checks	detect spammers & botnets
▪ Content checks	ClamAV & SpamAssassin
▪ Manual inspection queue	suspected phishing & malware

Filter Components (first-generation filter)



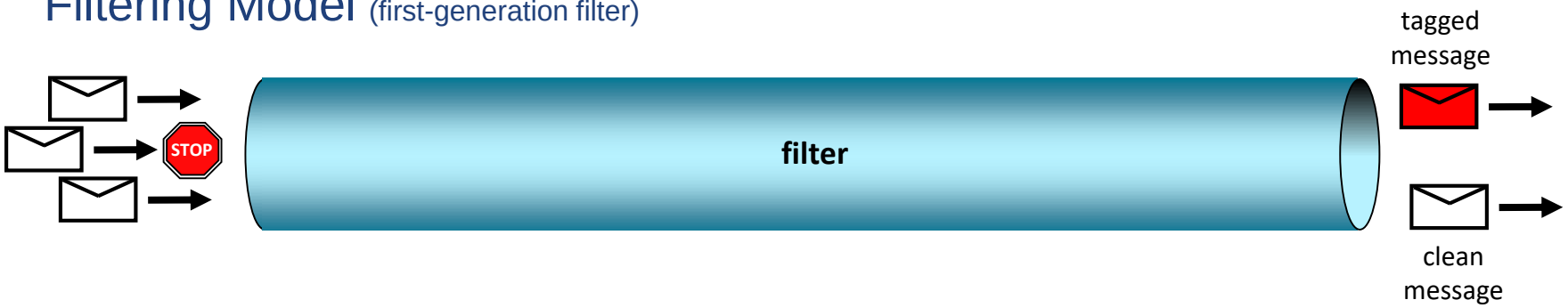
Filtering Checks (first-generation filter)

- Sender IP-address reputation
- HELO string analysis



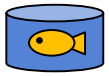
- Sender domain check
- Recipient address check
- Personal black-lists & white-lists
- Message content analysis

Filtering Model (first-generation filter)



- Junk messages are rejected at SMTP-time (default action)
- Messages from bad senders may be rejected without checking the content
- Users are provided with a personal **blacklist** & **whitelist**
- Users are provided with a **tag-only** option for spam
- Requires special handling of messages with multiple recipients
- Confirmed malware & phishing messages are rejected
- Suspected malware & phishing messages may be held for inspection

The “Phish-Trap” Inspection Queue



- rules to detect phishing & executable content
- we deleted about 90% of the queued messages
- message inspection eventually took up to 4 hours/day
- 1.5 million messages/year landed in the queue
- rules & exceptions required frequent updates
- messages remained in the queue over-night & over week-ends
- users complained about delivery delays & privacy

By 2016, we found the first-generation filter to be inadequate

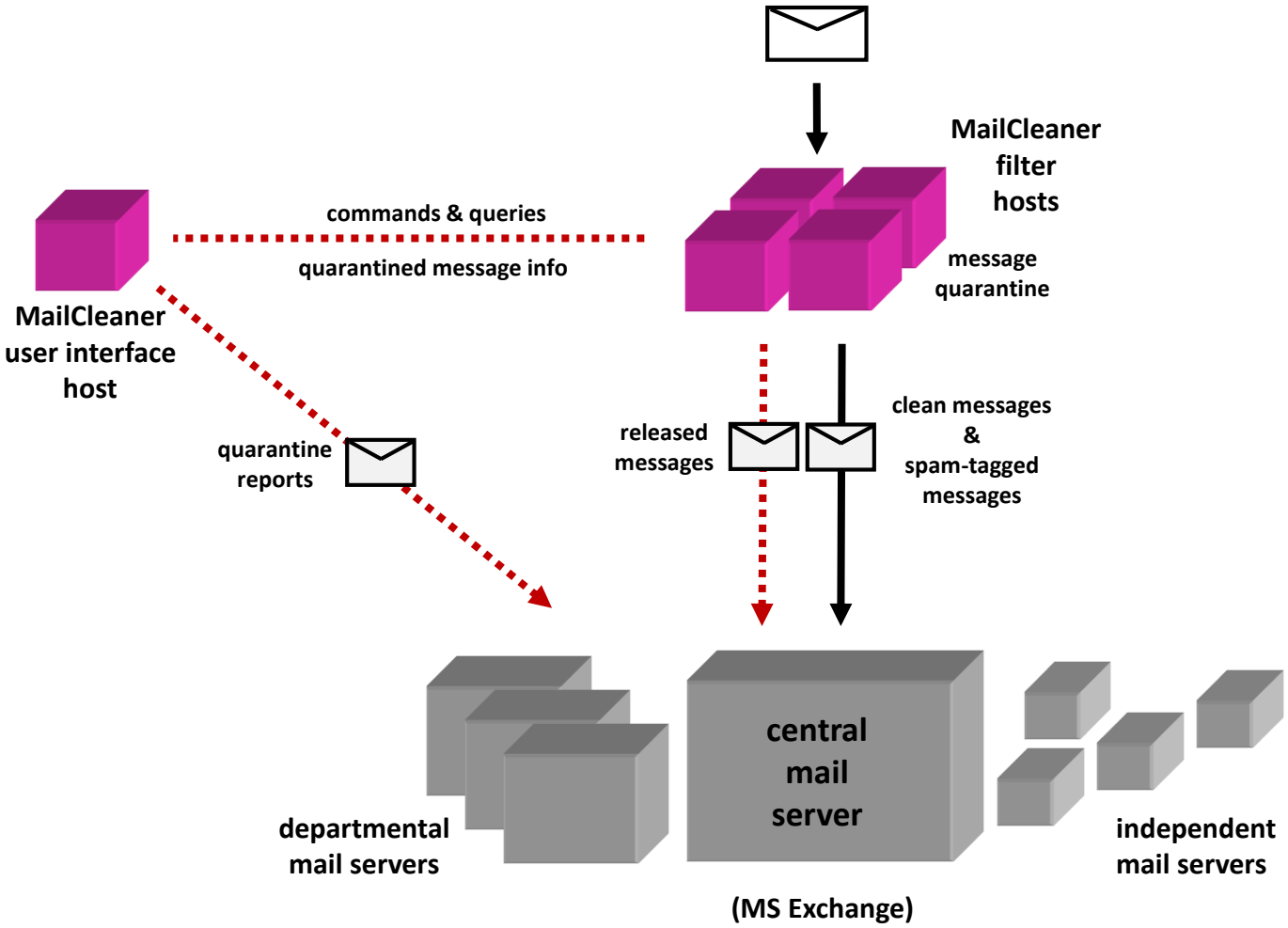
We needed:

- new versions of software components
- more filter checks
- an additional anti-virus component
- a better way to report positives & false negatives
- an alternative to the phish-trap

MailCleaner

- provided by Fastnet SA, a Swiss company
- installed on our local servers
- already in use at various Swiss universities

Filter Architecture



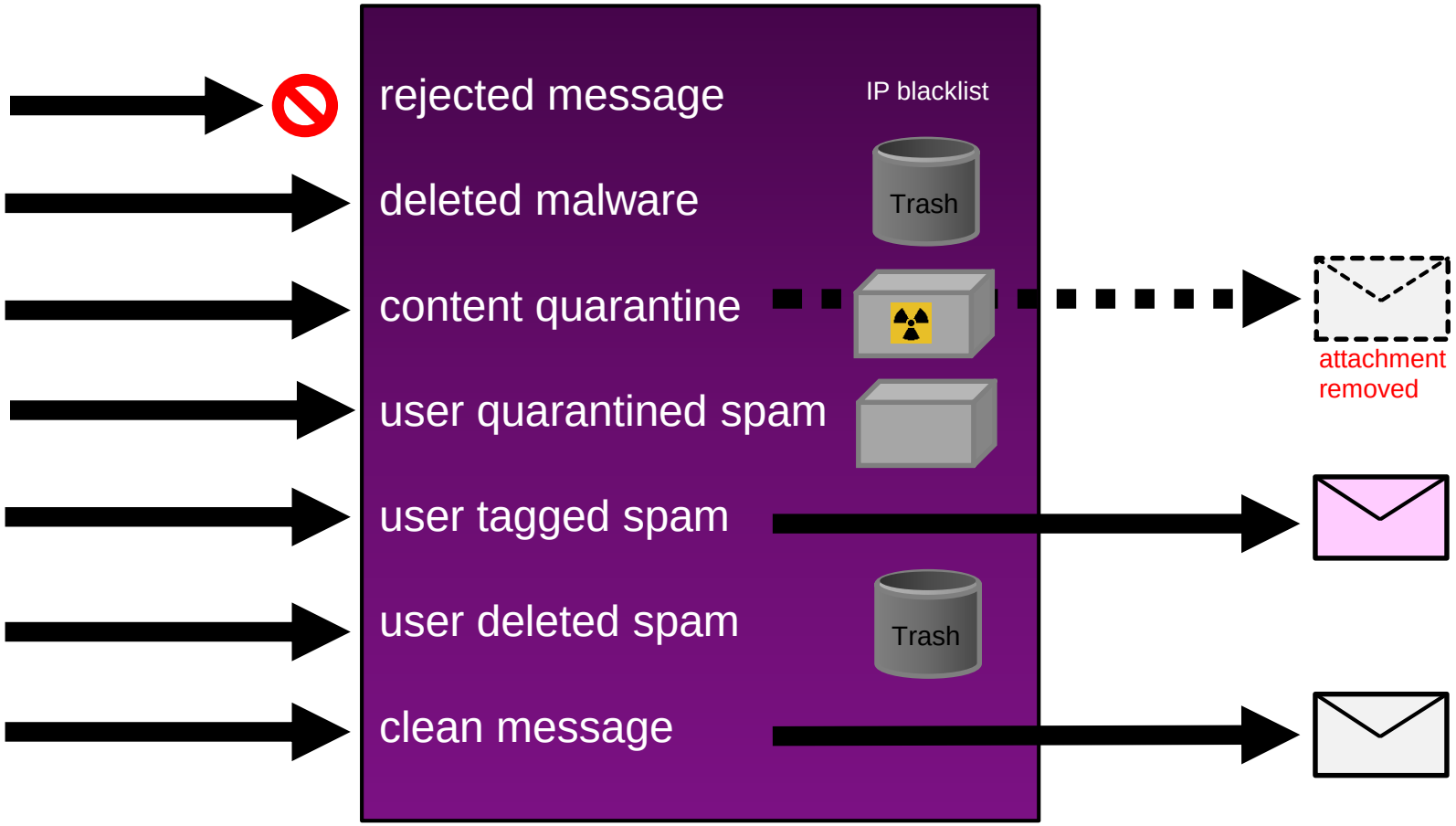
MailCleaner - features

- filter out spam, fraud, phishing & malware messages
- filter out unwanted newsletters
  - spam disguised as a newsletter
  - malicious newsletter subscriptions
- personal quarantine (30-day)
  - reports per e-mail (daily, weekly, monthly)
- web-based user interface
  - uses your ETH mail username & password
  - reporting & filtering preferences
  - black/white/warn lists
  - newsletter whitelist

MailCleaner

- open source software components (exim, spamassassin, etc.)
- commercial blacklists
- open source & commercial anti-virus components
- rule-based filtering & bayesian filtering
- mechanisms to report false-positives & false-negatives
- FP/FN reports are used to update the bayesian filter (automated process)
- FP/FN reports are used to create filtering rules & anti-virus signatures

MailCleaner – filtering model



MailCleaner – headers added to filtered messages

When reporting a message back to MailCleaner, these headers help the company to understand why a message was wrongly classified

X-MailCleaner-SPF: pass

From: Nomasis NEWS <Nomasis.NEWS@nomasis.ch>

X-Newsl: is newsletter (6.0/5.0)

X-NiceBayes: is not spam (29.04%)

X-Spamc: is not spam (score=2.0, required=5.0)

X-MailCleaner-Information: Please contact servicedesk@id.ethz.ch for more information

X-MailCleaner-ID: 1hY3zF-0008Ba-TY

X-MailCleaner: Found to be clean

X-MailCleaner-SpamCheck: not spam, Newsl (score=6.0, required=5.0,
MC_EN_UNSUBSCRIBE=1, MC_NEWS_ENWNEWS=1, MC_NEWS_HFRMNEWS=2,
MC_NEWS_URIUNSUB=2), Spamc (score=2.0, required=5.0,
RCVD_IN_DNSWL_NONE -0.0, T_FRT_CONTACT 0.0, URIBL_BLOCKED 0.0,
HTML_FONT_LOW_CONTRAST 0.0, BAYES_50 0.0, HTML_MESSAGE 0.0,
MC_MAILTO_WITH_SUBJ_ORDER 2.0, FILL_THIS_FORM 0.0)

Subject: Nomasis Webinar

X-MailCleaner-ReportURL: https://mailcleaner.ethz.ch/rs.php

MailCleaner – providing feedback

- report false positives
  - quarantine filter-adjustment icon 
  - nospam@ethz.ch — a forward to nospam@mailcleaner.net
- report spam
  - spam@ethz.ch — a forward to spam@mailcleaner.net
- report phishing & malware
  - phishing@ethz.ch — notifies the Informatikdienste
  - virus@ethz.ch — & the MailCleaner team
- To include the message headers, *send the mail as an attachment*

MailCleaner – how feedback is used

- Reported messages are fed into a Bayesian classifier
  - Adjustments are *incremental (like an «up» vote or «down» vote)*
  - Adjustment requests may need to be repeated over several days
- Messages are sent to the MailCleaner analytical team & to our ticket system
- We may remove phishing/malware messages from mailboxes or block the sender
- Messages may be used to create filtering rules & anti-virus signatures

Problem Areas

- We cannot react instantly to phishing/malware attacks
  (no 24/7 operations room at ETH or at MailCleaner)

- Distribution lists require special handling to prevent delivery of quarantine reports to all list members

- Our account provisioning system does not manage MailCleaner user/address profiles

Problem Areas

- We have no mail client plug-in to report spam
- Users do not forward undetected spam back to the company
- Users fail to forward undetected spam *as an attachment*
- Outlook removes X-headers from forwarded messages

User Expectations about Mail Filtering

- Unrealistic & often irrational
- E-Mail is seen like “instant messaging”
- Users will not tolerate delivery delays
- Users have a low tolerance for false positives or false negatives
- Some users feel that they are too important to manage their own white/blacklists or even to look into their quarantine
- Users want complete privacy (no other human should look at their mail)

Criminal Activties – 2020

- malware & spyware
- extortion using ransomware
- CEO Scam
- bank account scam
- iTunes scam
- user-account phishing
- financial-account phishing

Malware

- Ransomware – block computer access or encrypt your files sometimes combined with threats to reveal sensitive information
- Spyware − espionage by criminals & foreign governments
- Botnet – use your computer for mail or DDos attacks
- Cryptojacking − use your computer for bitcoin calculations

More about Scams

- CEO Scam
  - mail from “the boss” claims that your company is making some **secret** deal and asks you to authorize a payment to some account
  - often combined with a telephone call from a “lawyer” or “bank” demanding immediate action
  - this scam requires knowledge about the CEO’s travel plans

More about Scams

- bank account scam
  - mail comes from one of your “suppliers” saying that their bank account changed
  - scam requires knowledge about your suppliers

More about Scams

- iTunes gift card scam
  - mail from “the boss” asks you to buy gift cards, reveal the redemption code, make a photo with your phone and send the photo to some telephone number
  - scam requires knowledge of your organization
  - information about the ETH is provided by departmental web pages and by the “Advanced search options” offered by the ETH Homepage

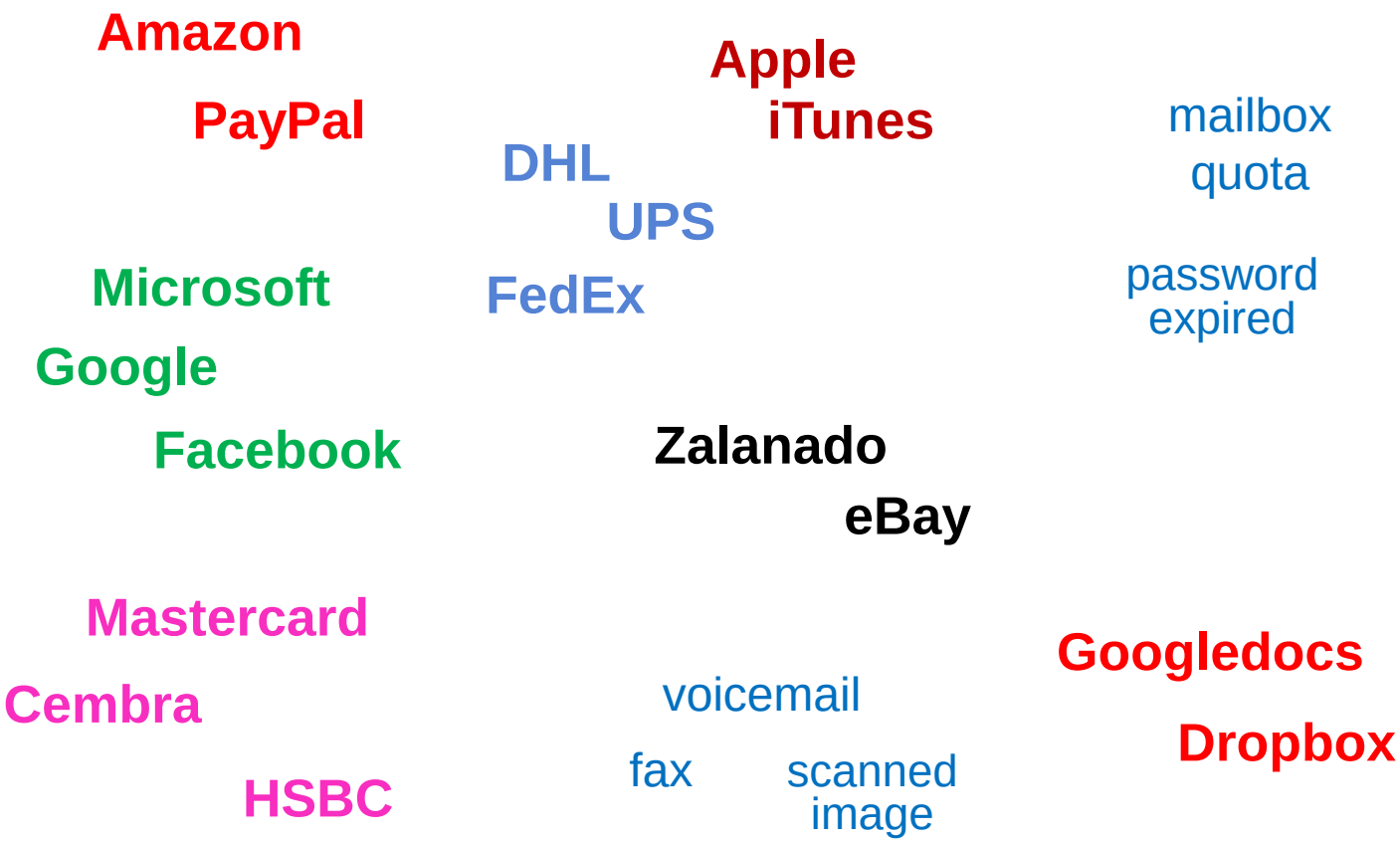
Other spams & scams

- Spam disguised as a newsletter
- Malicious subscription to newsletters
- Open-access journals
- Fake conferences
- Sex-site blackmail
- Political spam

Evil messages that are difficult to catch

- Order confirmation from an on-line shop
- Phishing that targets a single person
- Message with a sabotaged attachment (pdf, docx, xls, etc.)
- Encrypted or polymorphic malware
- Invoices
- Document to view or sign
- Minimal text + URL
- Image + URL

Generic phishing & malware messages



Regional phishing & malware messages

UBS

ZKB

Ricardo

UZH

Postfinance

ETH

Swisscom

Migros

Coop

Digitec

Brack

Thematic phishing & malware messages

COVID-19 Tracing notifications

ZOOM meeting

MS Teams meeting

University phishing messages.

- user account verification/update
- mail quota exceeded
- fake security update
- your user account is hacked
- virus found in your mailbox
- you have quarantined messages
- blackboard (education sharing service)
- new library resources
- veranstaltungs kalender
- student grants/loans
- update your ETH password

Simple Phishing Attack – November 2018

From: “ETH Zurich” <admin@patrik.com.ua>
Subject: You’ve Got Mail!

Dear User,

This is to notify you of an important meeting.

Click here for details

Thank you.
ETH Zurich

Sophisticated Malware Attack – September 2019

- Inboxes were copied from compromised external accounts
- Messages were sent to our users as replies to mail that our users had previously sent
- Messages contained a .doc attachment with a macro to download malware
- Attachments had already been tested against anti-virus products
- Random addresses used in the envelope-sender address & From: headers
- Display names & signature blocks contained info from our users or their correspondents

Phishing & Malware Countermeasures

- To limit the number of messages sent from a compromised account, we limit the number of messages that can be sent by a user in one day
  - our limit is 500 messages/day
  - one Swiss university sent 11 million messages from a compromised account
- Filter updates – based on received mail
- Remove phishing/malware messages from user mailboxes
- Lock accounts that send evil messages or host a phishing web page
- Neutralise phishing URLs
  - Redirect a phishing URL to a warning web page
  - Block a phishing URL's IP-address