Phishing, Pharming, and Phraud: The Joy of Phighting Email Spam

René Wienholtz
(CTO, STRATO Rechenzentrum AG)
What makes Spam fighting a „real joy“?

STRATO, AntiSPAM & Research – why?

Findings of the past...

Future research topics...

Join us!
Spam – a “real joy”?

...yes, if you look at these fine pieces of art:

Spam rhymes (German):

- Wer abends mit der Pille wurzt, sich nachts auf seine Alte stürzt!
- Nimm die Pille, sei kein Dummer, sonst schaffst du nie 'ne gute Nummer!
- Wird er im Alter manchmal weich, nimm die Pille, dann steht er gleich!
- Nimm die Pille, sei kein Tor, dann steht er wie ein Ofenrohr!
...yes, if you look at these fine pieces of art:

```
Received: from 192.168.0.%RND_DIGIT
 (203-219-%DIGSTAT2-%STATDIG.%RND_FROM_DOMAIN
 [203.219.%DIGSTAT2.%STATDIG]) by mail%SINGSTAT.%RND_FROM_DOMAIN
 (envelope-from %FROM_EMAIL) (8.13.6/8.13.6) with SMTP id
 %STATWORD for %TO_EMAIL>; %CURRENT_DATE_TIME
Message-Id: <$RND_DIGIT[10].%STATWORD@mail%SINGSTAT.%RND_FROM_DOMAIN>
From: "%FROM_NAME" <$FROM_EMAIL>
%TO_CC_DEFAULT_HANDLER
Subject: %SUBJECT
Sender: "%FROM_NAME" <$FROM_EMAIL>
Mime-Version: 1.0
Content-Type: text/html
Date: %CURRENT_DATE_TIME

%MESSAGE_BODY
```

THIS IMAGE PASSED THROUGH ALL FILTERS SO YOU OUR POTENTIAL CUSTOMER COULD HAVE AN OPPORTUNITY TO KNOW ABOUT OUR GREAT SERVICES AND PRODUCTS.

YOU HAVE AN OPPORTUNITY TO ORDER DIRECTLY FROM OFFSHORE MANUFACTURERS

VIAGRA 100MG $2.81
VIAGRA (SOFT) 100MG $3.51
CIALIS 20MG $3.46
CIALIS (SOFT) 20MG $3.55
PROZAC 60MG $1.99
LEVITRA 20MG $3.97
**STRATO:**
- since 1998
- Products: Shared-WebHosting, Dedicated Servers, Shop Platforms, DSL
- pan-European: DE, ES, FR, IT, NL, UK

**Why a research project for AntiSPAM/Phishing?**
- Focus on Ham, Resource optimization
- Discovering spoof-poof filter methods
- Use of machine-learning aspects with less manual training and QA
- Handling of Outbound-/CGI-Spam
Using the social network theory...

- Has a communication already been established before and how strong is the social relationship?
- How likely is it, that A has an intention to send an email to B (or others)?
- Works a bit like a DCC data repository

DB stores irreversible hash values

- Fine for minimizing the false positive rate
- Quite spoof-proof method

Further developments:
- Evaluation of 2nd / 3rd level relationships
- DB need more input for even better accuracy

Hash-Value Database

No: enter value into DB and set counter to 1
Yes: lookup value, report counter to filter engine & raise counter by 1
Using Image Fingerprinting / Batch Recognition...

- Finding similarities in Emails and attached Files
- Generates unique feature combinations
- Used first in detecting image batches
- Has much less performance impact than e.g. OCR but is also more accurate

Works not only for images but also for text content and other media types (Movies, PDF etc.)
Future research topics...

 ► **Personalized filter training...**
   - Optimizes the filter accuracy especially for marginal groups, like Urologists chatting about Viiiiii\gra ;)

 ► **Autonomous filter tuning using games theory...**
   - Self-outsmarting filter for pre-training the classifier against new Spam methods

 ► **Generation of new statistical attributes...**
   - Soft-Blacklisting of servers and discriminative clustering of batch attributes

 ► **Integration of Botnet Data...**
   - Infiltration of Botnets and using drawn off data to tune the filters
We want to open a periodic German / European ISP roundtable for discussing Anti-Spam topics for “techies” (mail infrastructure administrators & developers)

The aim is to find projects like setting up shared databases & services, push new protocols etc. and to bring in new ideas

We’re already in contact with Freenet (of course;) and the United Internet group and we hope there are more to come...

For joining this group please contact:

isp_antispam at strato dot com

(Subject: Joining ISP Anti-Spam group...)

Rene Wienholtz:
Phishing, Pharming, and Phraud
Thank you for your attention...

René Wienholtz
STRATO Rechenzentrum AG
Pascalstrasse 10
10587 Berlin
GERMANY