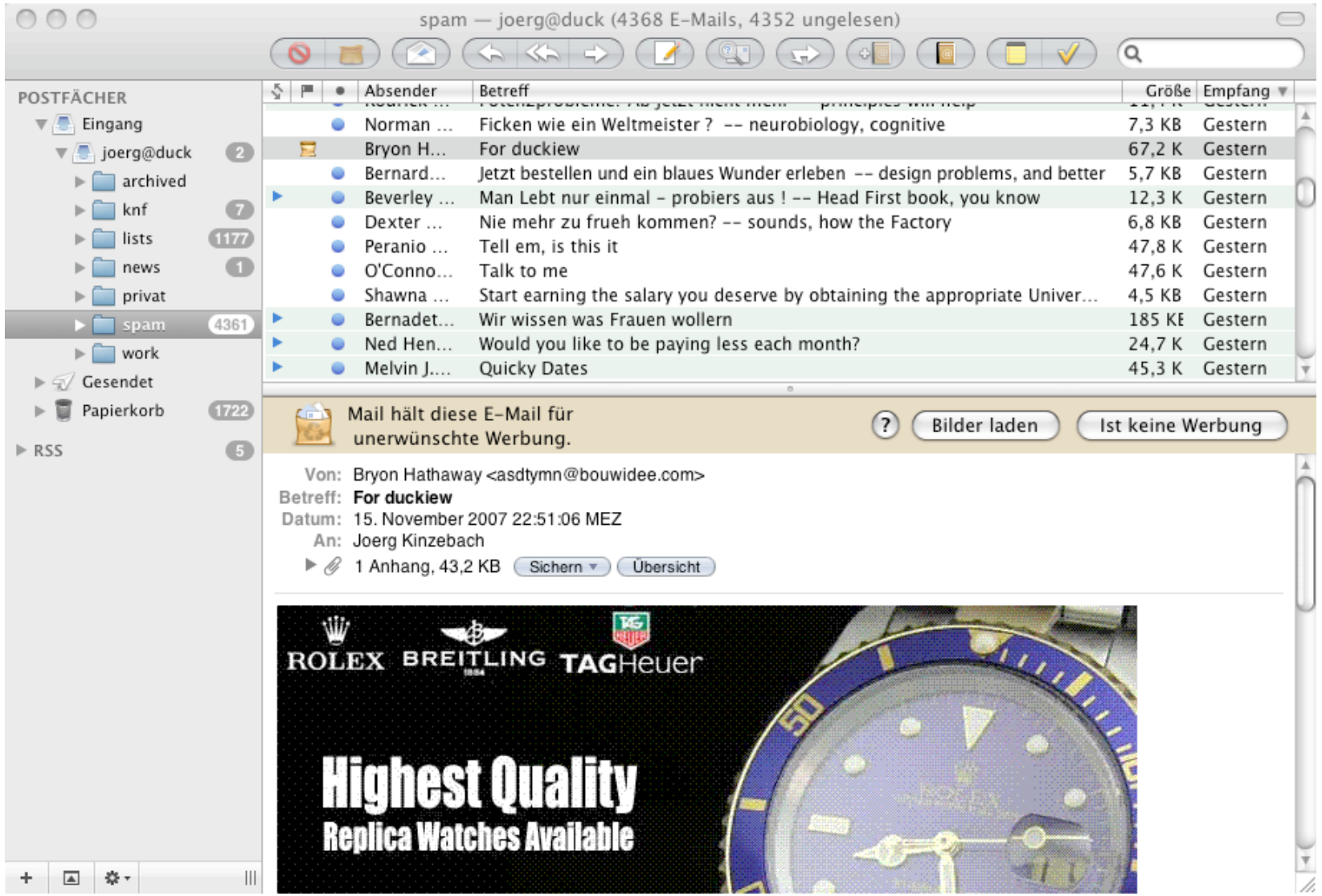
Spam

im Wandel der Zeiten

Jörg Kinzebach <joerg@duck.franken.de>

... täglich in den Posteingang



... geändert hat sich

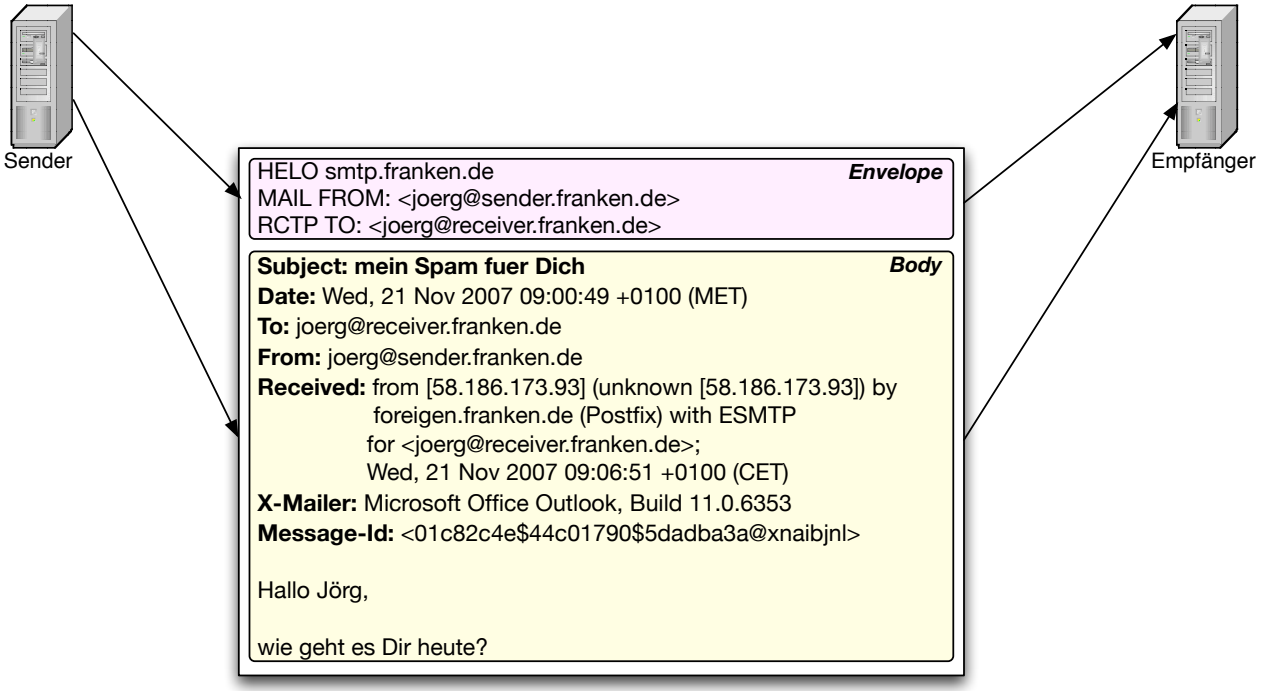
- Volumen
  - Größe der Mails
  - Anzahl der Mails
- Quelle für Zieladressen
- Verbreitungswege

- Filtermöglichkeiten
- benötigte Resourcen für Mailbetrieb

Ein "Business" nicht nur für Spammer

- Platten-Verbrauch steigt erheblich
- Investitionen für Mailbetrieb
  - Abruf
  - Traffic
  - Annahme von Mails/Datenbanken
  - Filterung
- Appliances zur Spam-Filterung

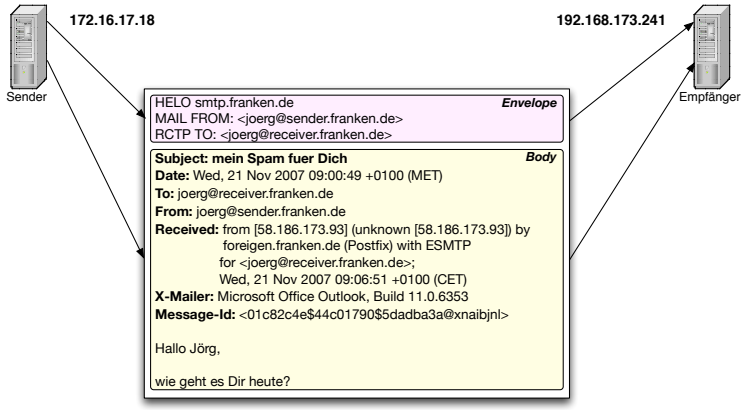
SMTP (Simple Mail Transfer Protocol)



- Mail besteht aus "Envelope" und "Body"
- Envelope ist kurz und man kann "schnell" und "resourcenschonend" filtern
- Body enthält viele Hinweise auf Spam

Filtern auf den Header

- Verfügbare Informationen:
  - Einliefernde IP-Adresse
  - Absender Hostname im "helo" bzw. "ehlo"
  - Absender-Adresse
  - Empfänger-Adresse
- Filtermöglichkeiten:
  - Kommt die Mail aus einem "unerwünschten" Land?
  - Existiert Absender-Adresse?
    - Domain im DNS zu finden?
    - Verification-Callout?
  - Einliefernde IP bekannt als Spam-Quelle? (RBL)
  - Absender-Adresse bekannt als Spam-Quelle (RBL)
  - Darf Absender-Adresse vom Quell-IP kommen? (SPF)
  - Greylisting (Einlieferer zu einer wiederholten Einlieferung zwingen)



Filtern auf den Body

KNF

- Schlagwörter (Viagra, Online-Casino, Penis-Enlargement)
- Variationen von Schlagwörtern (Obfuscation, z.B. "V!agra")
- Fehler in der Mail (defekte Header-Zeilen, falsches Encoding, HTML-Fehler, X-Mailer setzen aber falscher Algorithmus um Message-ID zu erzeugen)
- Pfad der Mail (Überprüfung von Received-Zeilen)
- HTML-Inhalt
- Bild-Anzahl und Grösse
- Links auf bekannte von Spammern begünstigte Web-Shops (SURBL)
- Hashes des Mailtextes erstellen und vergleichen um massiv häufig eintreffende Mails zu erkennen (Razor, Pyzor, DCC)
- Bayes (Text-Analyse, erlernen welche Wörter nur in "guten" Mails und welche Wörter hauptsächlich in "schlechten" Mails vorkommen)
- Bilder- und PDF-Untersuchung (FuzzyOCR, Checksumming)

Was haben Spammer gelernt

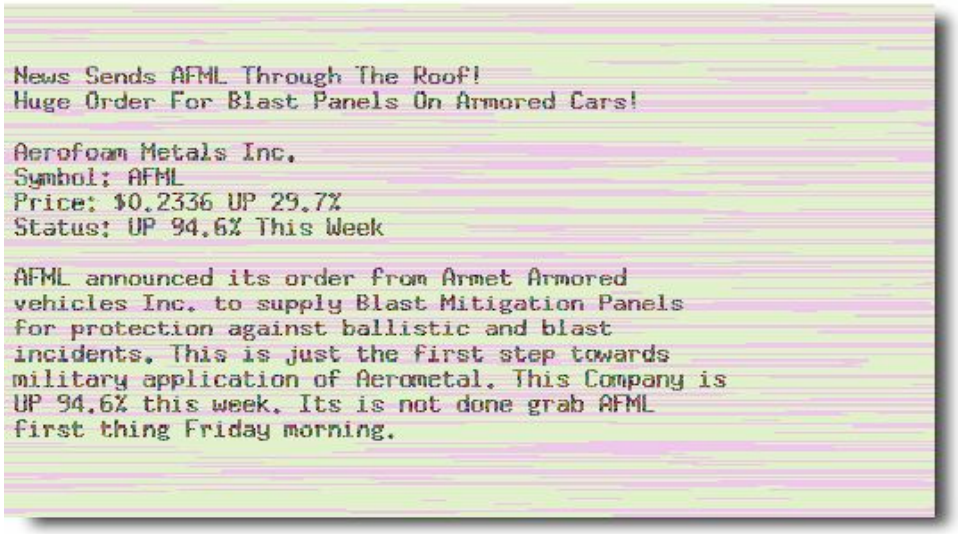
KNF

- nicht selbst versenden, das wäre zu einfach zu filtern
- nur existierende Absender-Adressen/Domains verwenden
- Schlagwörter nicht im Klartext verwenden
- Syntax-Fehler in Mailheadern vermeiden
- keine HTML-only Mails verschicken
- Wechsel des Inhalts der Mail schnell vollziehen, bevor die "Welle" bekannt ist
- Personalisierung der Mails
- SPF auf Absender-Domain setzen
- Text ohne Spambezug in die Mail einarbeiten um Bayes-Filter zu umgehen
- Wiederholung der Auslieferung um Greylisting zu umgehen
- Sende-Systeme bevorzugen, die nicht in Blacklisten stehen
- Spam-Text in Bilder auslagern

Image-Spam

- Reine Body-Filter sehen die Reizwörter nicht mehr, der Empfänger sehr wohl
- Texterkennung (OCR) um Reizwörter in Bildern zu finden: sehr aufwendig
- Prüfsumme der Bilder um Massenspam zu erkennen

Image-Spam TNG



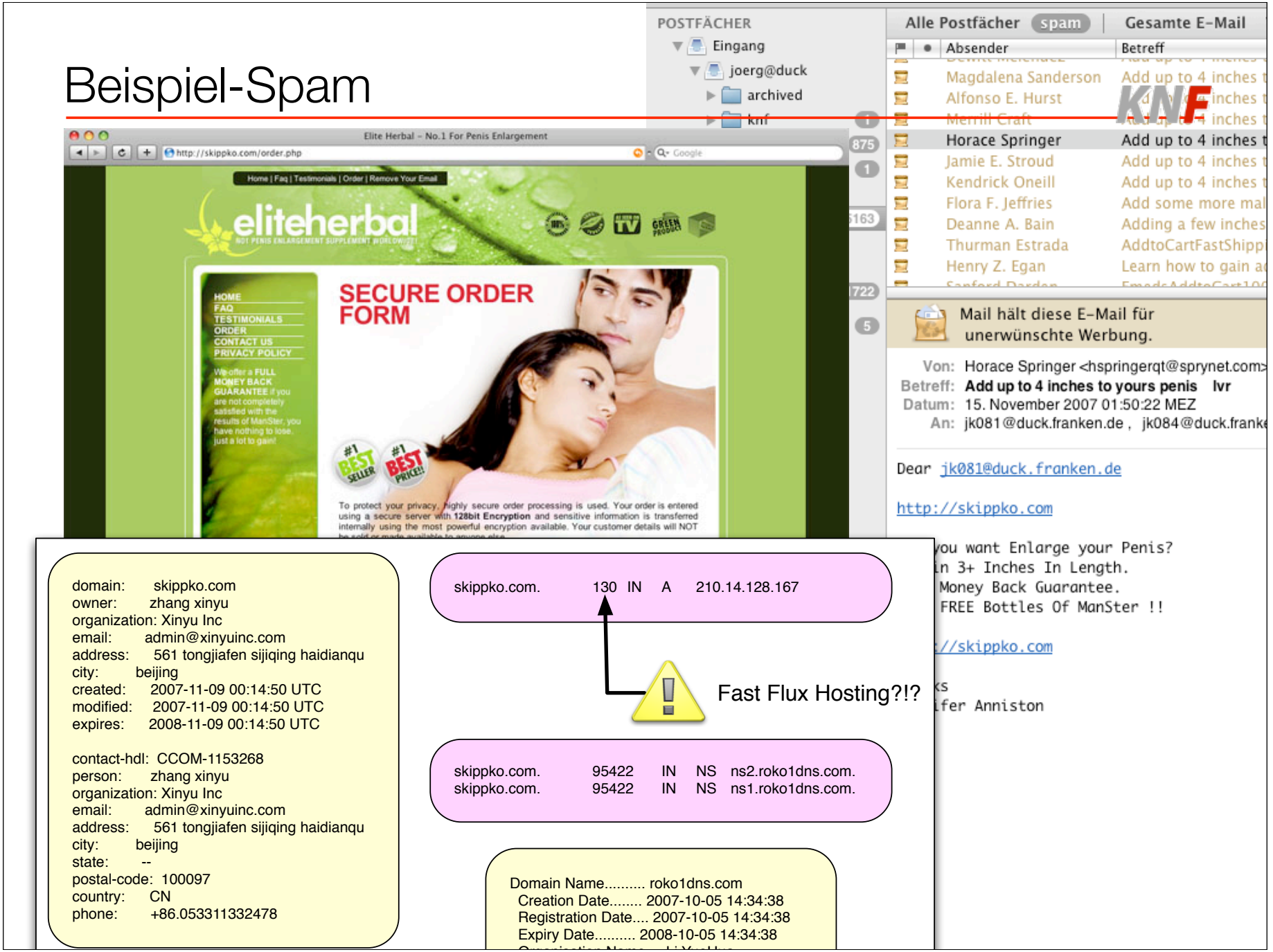
- Zufallspunkte oder Striche im Bild um Vergleich von Checksums/Hashes zu erschweren (Erkennung von Massenversand des gleichen Bildes)
- Verwendung von Zeichensätzen, die automatische Texterkennung erschweren
- gezielte Störungenen im Bild um Texterkennung unmöglich oder zumindest teurer zu machen

Spam-Ziele

KNF

- Verkauf von Produkten
  - Viagra
  - Tintenpatronen
  - Markenimitate
  - mindersensibilisierte Kleingewerbetreibende
  - Porno
- Aktien-Spam
- Phishing
  - Konto-Daten
  - Account-Daten
    - Server (Webserver, Shell, E-Mail, Ebay)
    - Multiplayer Online Gaming
  - Persönlichkeitsdaten
- Vergrösserung des Bot-Netzwerks

Beispiel-Spam



Herbal King

- Neuerdings auch als Elite Herbal unterwegs
- Ursprung: Indien
- Hunderte bis tausende verschiedene Domains
- Beworben werden hauptsächlich Penis-Enlargement- und andere Medikamente aber auch Porno-Seiten
- Grösstenteils gehostet bei vor Zugriffen geschützten Hostern in China, aber auch Fast-Flux
- Spam wird über Bot-Netze versendet
- Steht in Konkurrenz zu den traditionell von Osteuropa ausgehenden Spam-Gangs

Pump and Dump (Stock Spam)

GOLDMARK INDUSTRIES, INC. (GDKI)

Sent: Wednesday, December 20, 2006 2:32 AM
Subject: send-off disposal

GDKI IS MAKING EVERYONE BANK!

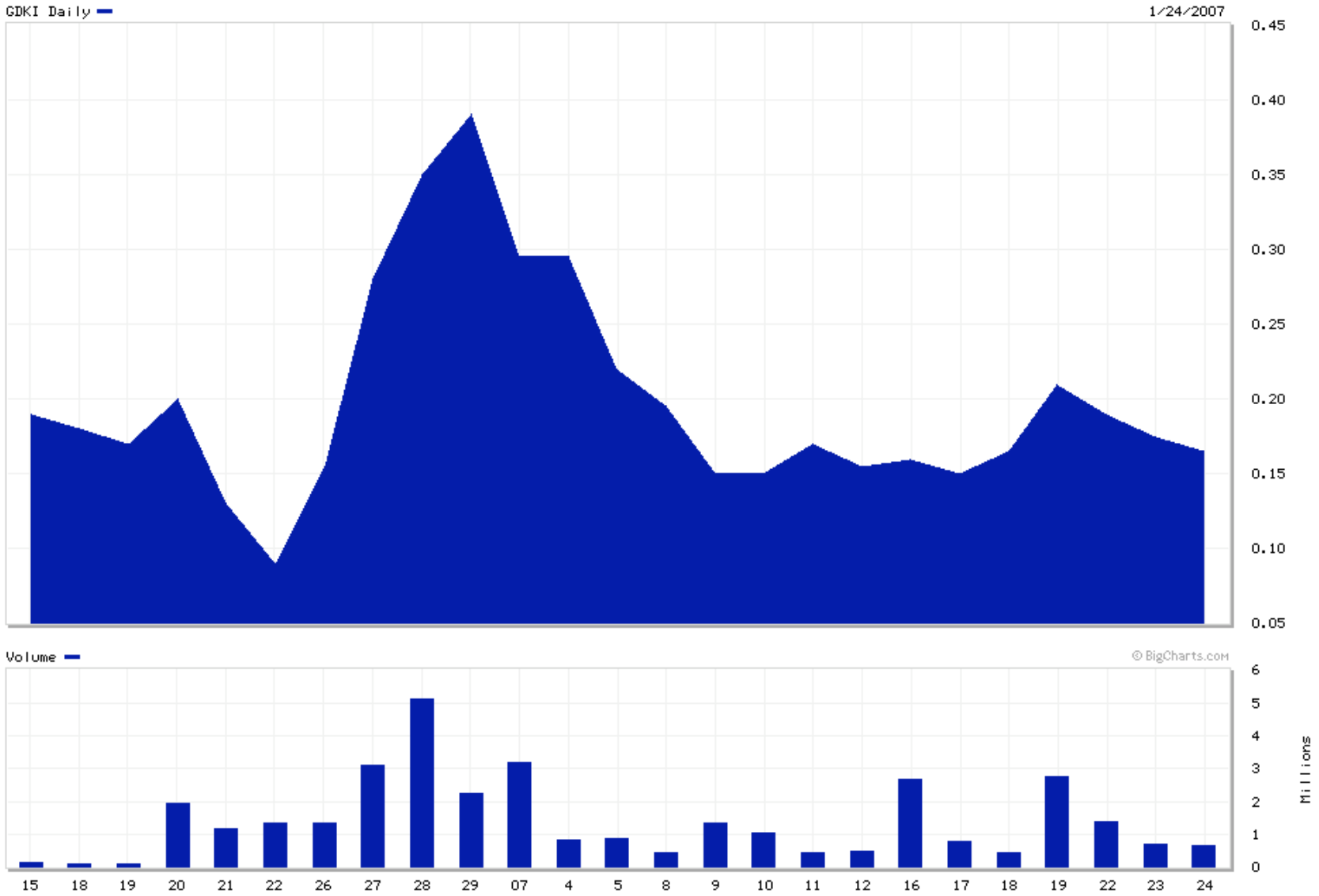
Trade Date: Wednesday, December 20, 2006
Company: GOLDMARK INDUSTRIES (Other OTC:GDKI.PK)
Symbol: GDKI
Price: $0.17
5-day Target: $2

DON'T LET THIS OPPORTUNITY PASS YOU BY! WATCH GDKI SOAR ON WEDNESDAY DEC 20!

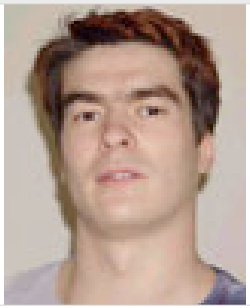
Wall Street Technology Jobs - New York Financial District Technical Careers in Equity Trading, Stock Markets, and Financial Services.
Your skills and qualifications are evaluated and if your background meets the job requirements of one or more of our client companies, we will contact you within a day or two. Experience building real-time add-ins. Advanced SQL programming experience. If that describes you, we'dlike to hear from you. However, we will keep your resume on file, in the event a suitable position arises.

- 19. Dezember 2006 GDKI bei Börsenschluss 0,17 $ und einem Volumen von 126.286 Aktien
- 20. Dezember 2006 beginnt Spam-Welle mit "Werbung" für GDKI Aktien
- 28. Dezember 2006 closed bei 0,28 $ und einem Volumen von mehr als 5 Mio
- 9. Januar 2007 Schlusskurs bei 0.15$

GDKI


GDKI Daily
1/24/2007
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0.10
0.05
Volume
© BigCharts.com
6
5
4
3
2
1
0
Millions
15
18
19
20
21
22
26
27
28
29
07
4
5
8
9
10
11
12
16
17
18
19
22
23
24

Bekannte Spammer

Alan Ralsky	Alexey Panov	Michael Lindsay	Leo Kuvayev
			
USA	Russland/Deutschland	USA	Russland/USA
• Spam-Sending via Dialup • Spam-Network • Rapid-Flux Spam Sending and Hosting	• Spam-Server • Hosting-Services für Spam • Vertrieb von Spam-Software	• Adress-Handel • Spam-Server • Botnetz-Betrieb	• Handel mit Spam-Servern • Vermietung von Spam-Servern • Raubkopien von Software • Porno, Arzneimittel • Phishing • Botnetz-Betrieb

Angaben von Alan Ralsky

- 1997:
  - Vertrieb über ein paar Mailinglisten: $6000 pro Woche

- 2002:
  - 250 Millionen gültige E-Mail Adressen
  - 0,25% der E-Mails erzeugten eine Reaktion
  - 0,75% der E-Mails wurden geöffnet (Tracking-Image u.ä.)
  - 89 Millionen Empfänger benutzten Opt-Out zwischen 1997 und 2002
  - bis zu $22.000 für eine einzelne Mail an alle Empfänger in der Datenbank
  - $750.000 mit einem Weight-Loss Spam verdient

Cyber Crime

- Preise für Daten und Dienste im Handel auf einschlägigen Platformen

Preis in US $	Dienstleistung/Produkt
1000-5000	Trojaner um Geld zwischen Konten zu transferieren
500	Kreditkartennummer inkl. PIN
80-300	Bankkonto, Adresse, SSN, Heimatadresse, Geburtsdatum
150	Führerschein oder Geburtsurkunde
100	Social Security Card
4-15	Kreditkartennummer mit Security Code und Ablaufdatum
2-5	PayPal Anmeldedaten

Unterwelt sehr öffentlich

KNF

From: <0x80@hush.ai>
Subject:VulnSale: IE 6.0.2900.2180.yeahlatestversion

So I just found another IE vulnerability. This time working on the latest patched up verison of 6.0. It allows for my code to be ran and all that pretty shit.

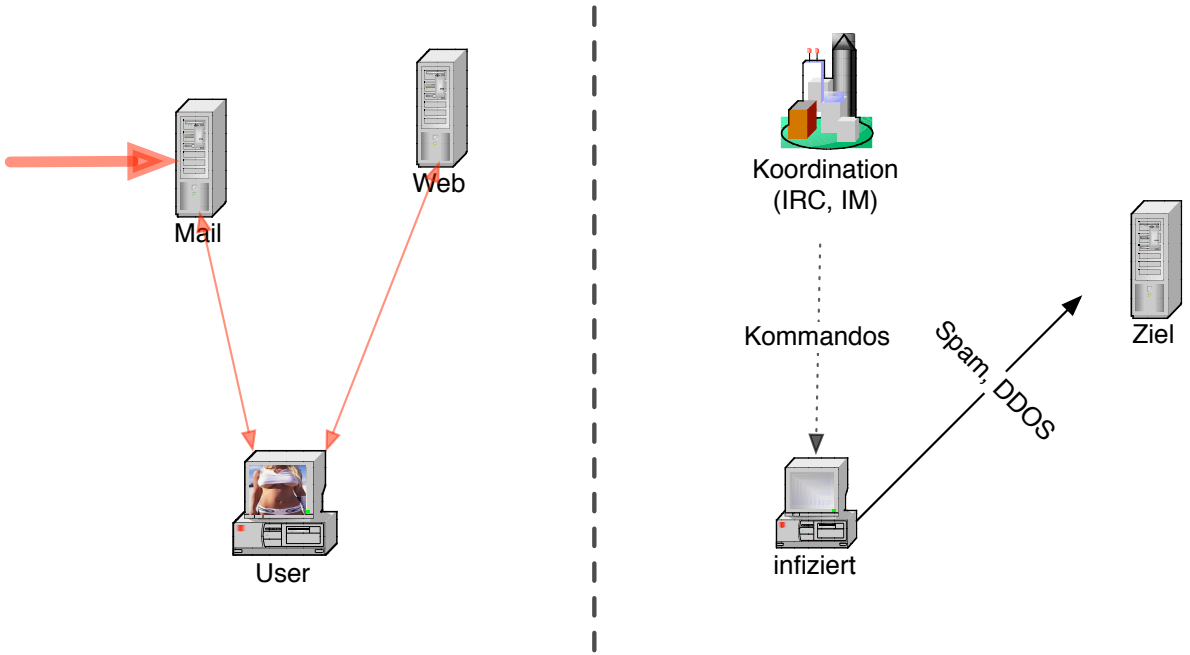
Let the bidding begin.

PS: Vista zero day sale ends Wednesday as I am already getting more bids than I can keep track of. For the sake of making a statement I have named the POC for this bug: litchfieldcantbypassaslrcauseheslame.c

-kkk

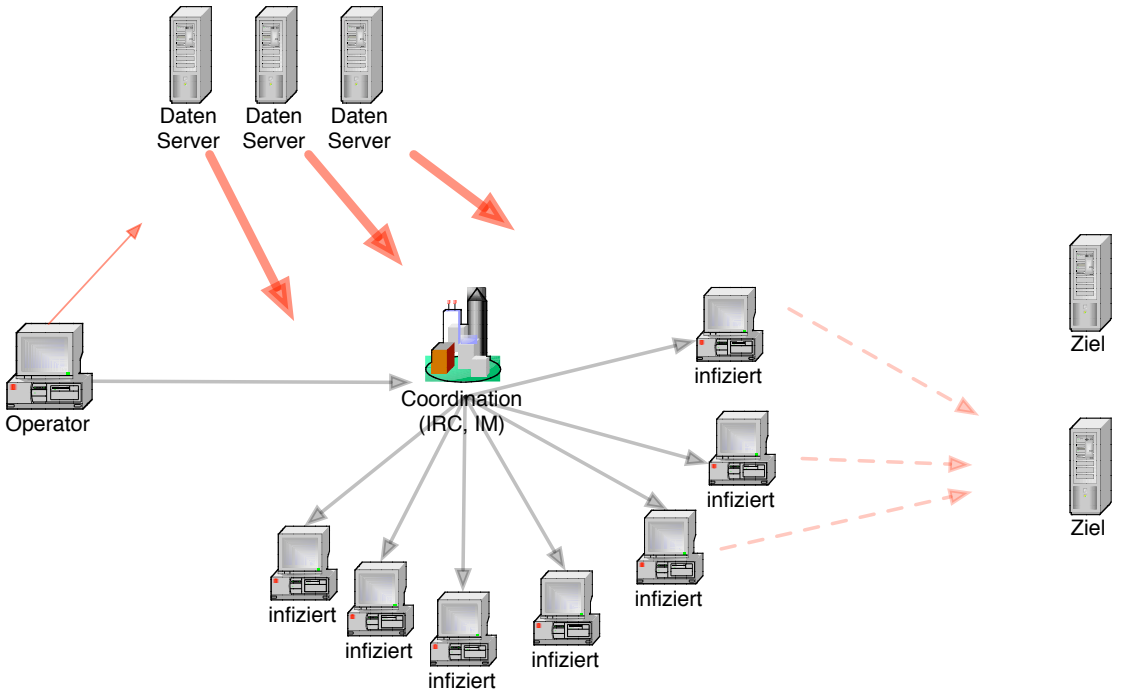
Bot-/Wurm-Infektion

- Infizierung durch E-Mail-Anhänge
- Infizierung über Webseiten/Exploits
- Installation eines beworbenen Programms
- Drohne verbindet sich nach Infektion mit einem Koordinierungsnetzwerk und wartet auf Anweisungen



Bot-Netzwerke

- Datenserver als Quelle für Informationen (Spam-Text, Adress-Listen usw.)
- unabhängiges Chat-Netz für Management des Drohnen-Netzes
  - Infrakstruktur bereits vorhanden
  - lässt sich nicht auf Botnetzbetreiber zurückverfolgen



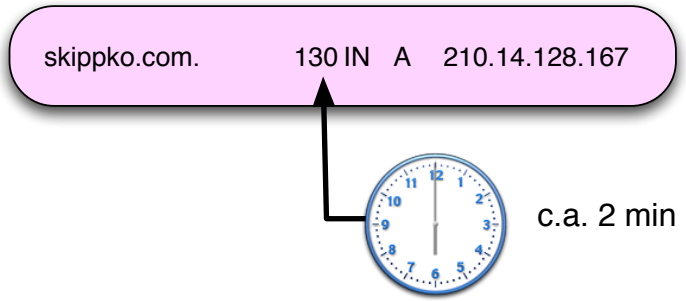
Bot-Netzwerke

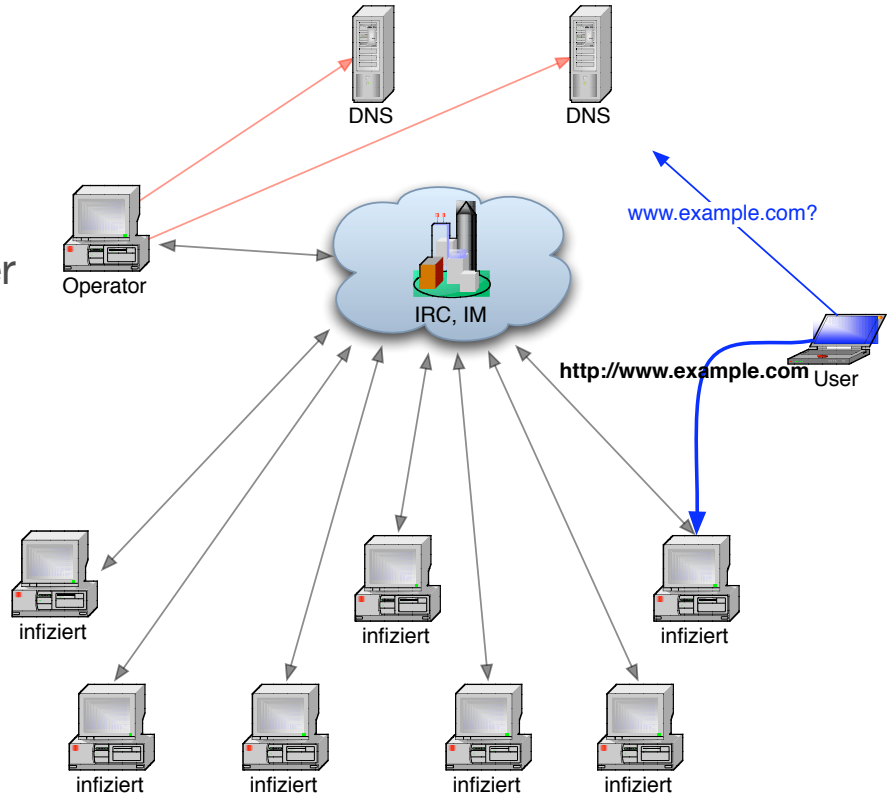
KNF

- selbst die kleinen Bot-Netze bestehen aus vielen tausend Drohnen
- teilweise wird mit mehreren millionen Drohnen geprahlt
- Aushebelung einzelner Drohnen zeigt wenig Änderung
- Tendenz zum Umstieg auf auf P2P-Netze um Single-Point-of-Failure zu vermeiden, sowie aus Performanzgründen
- heutige Drohnen sind eine Platform/ein Framework für verschiedene Anwendungen
  - FTP/Web-Server
  - Traffic-Erzeuger
  - IP-Forwarder
  - Shell-Server
  - Modular mit nachladbarem Code
- bei inzwischen verfügbaren Bandbreiten im Haushalt auf infiziertem Rechner kaum bemerkbar

Fast-Flux-Hosting

- Bot-Netz-Betreiber hat Zugriff auf viele Rechner mit hoher Bandbreite
- kurzlebige DNS-Antworten leiten Anfragenden auf einen infizierten Rechner, durch die kurze Haltezeit kann jederzeit auf einen neuen Rechner umgeschwenkt werden
- Ausfall einzelner Drohne (Abschaltung, IP-Wechsel, Infizierung erkannt) nicht signifikant im Gesamtnetz
- keine Daten auf eingenen Servern, Strafverfolgung wird erschwert, "abklemmen" nahezu unmöglich





Botnetz-Spammer: Vermietung des Netzes

```
>20-30k always online SOCKs4, url is de-duped and updated every
>10 minutes. 900/weekly, Samples will be sent on request.
>Monthly payments arranged at discount prices.
```

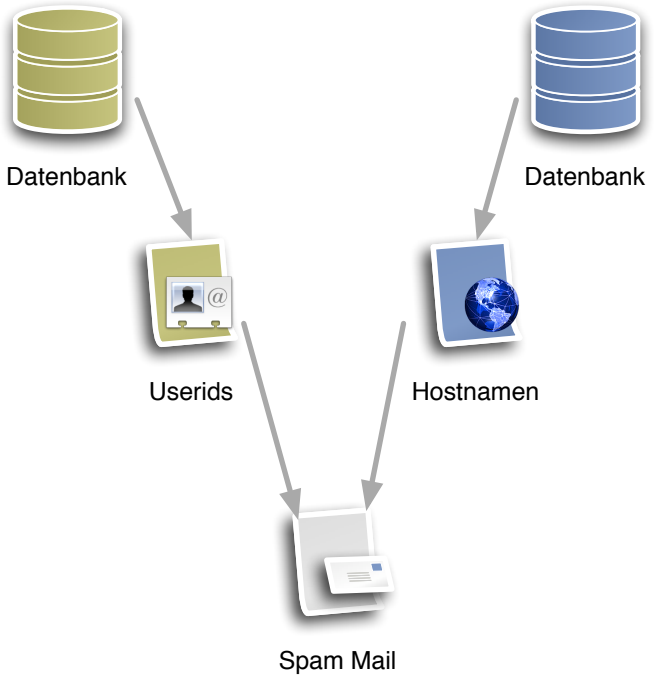
```
>$350.00/weekly - $1,000/monthly (USD)
>Type of service: Exclusive (One slot only)
>Always Online: 5,000 - 6,000
>Updated every: 10 minutes
```

```
>$220.00/weekly - $800.00/monthly (USD)
>Type of service: Shared (4 slots)
>Always Online: 9,000 - 10,000
>Updated every: 5 minutes
```

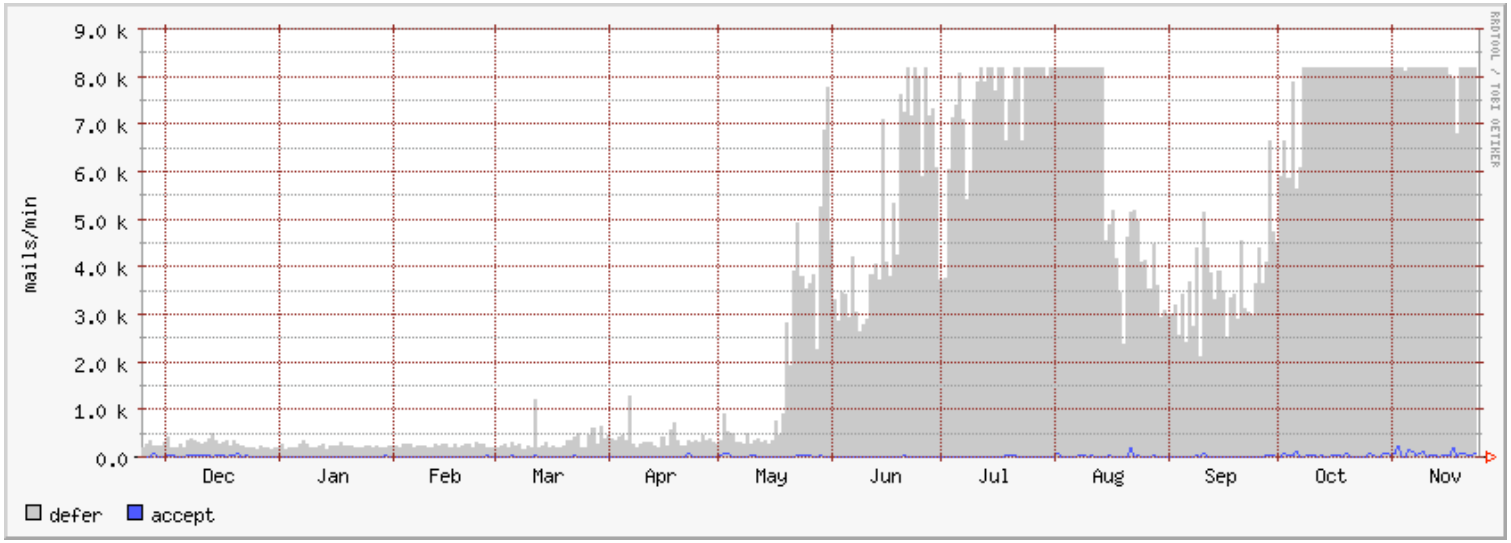
- 2-6 Cent (US) pro Bot pro Woche
- mehrere Nutzer eines Bots gleichzeitig möglich
- Nutzung als IP-Obfuscater via SOCKs

Dictionary-Attack

- Liste von Usernamen
- Liste von Domains
- Kombination von Usernamen und Domains erzeugt E-Mail-Adressliste
- Usernamen unter einer Domain existiert oft auch unter anderen Domain (Firmen, große Provider)
- Trifft auch unveröffentliche Empfängeradressen
- erzeugt regelmässig 500.000 Mails/ Auslieferungsversuche pro Domain pro Tag

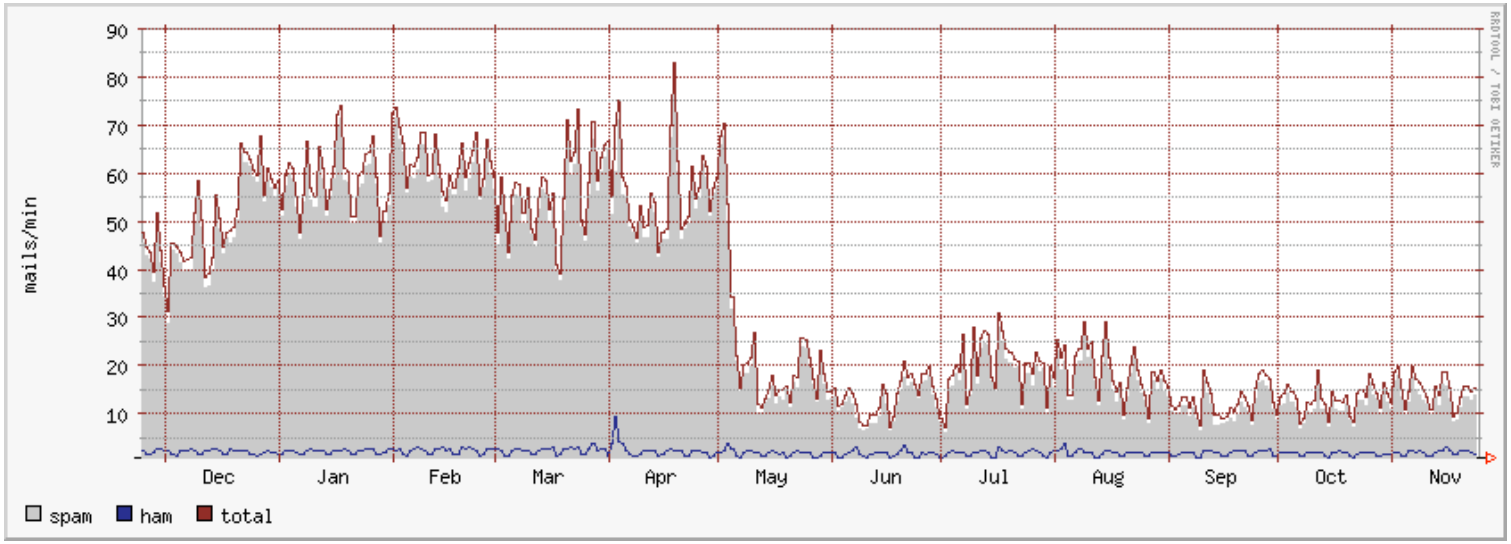


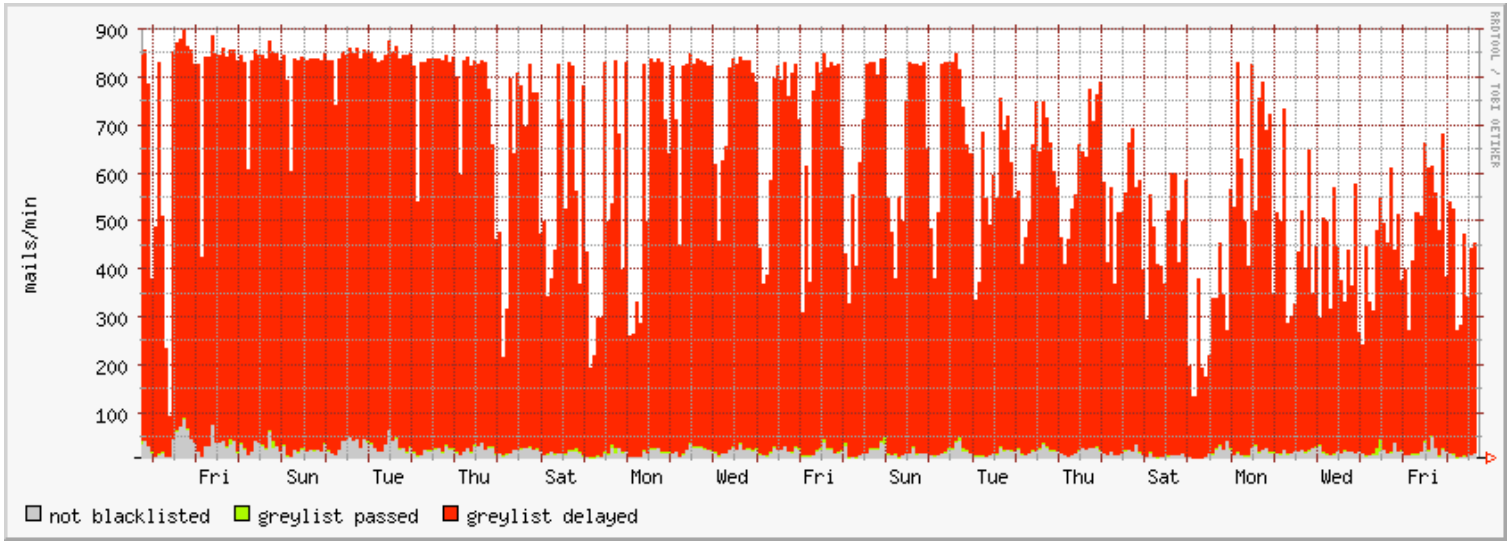
Mailmenge auf Backup



- Einlieferungsversuche explosionsartig gestiegen
- hauptsächlich "Dictionary-Attacks"

Mailmenge auf mail-n





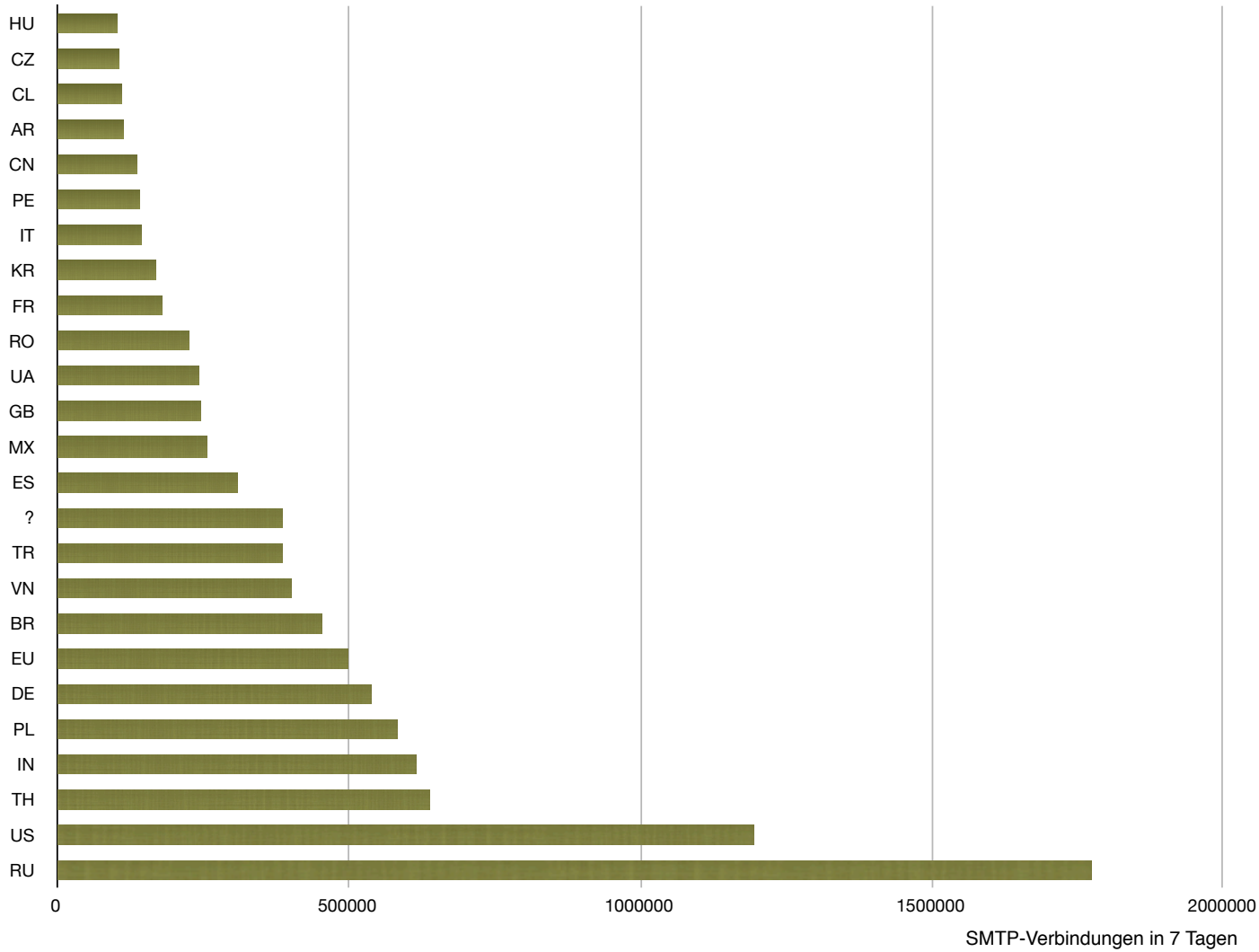
Taktik

KNF

- Dialup-IPs ohne Authentifizierung sind höchstwahrscheinlich Drohnen
- Durch Delaying von gelisteten IPs werden Drohnen ausgebremst und schlagen nicht bis auf den Filter oder Nutzer-Datenbank durch
- Da nur Delay und kein Blocking ist die Gefahr von "aus versehen" gelisteten IPs nicht zu groß, Mails kommen trotzdem an
- Blocken von allzu massivst einliefernden Ländern

Quellen von Mail-Einlieferung

HU	105.395
CZ	108.056
CL	112.929
AR	115.591
CN	136.661
PE	143.232
IT	146.061
KR	170.810
FR	180.980
RO	227.726
UA	244.610
GB	246.959
MX	258.923
ES	310.040
?	385.693
TR	387.932
VN	402.685
BR	454.913
EU	500.429
DE	540.262
PL	583.471
IN	616.137
TH	638.762
US	1.194.803
RU	1.774.110



vielen Dank für die Aufmerksamkeit

... noch Fragen?