Spam

Kein Schnee vom letzten Jahr

Jörg Kinzebach
<joerg@duck.franken.de>

Spam im Wandel der Zeit

- finanzielle Herausforderung
- Innovativer Werbung
- technische Herausforderung
- das Spiel mit dem Gegner
- Geld!

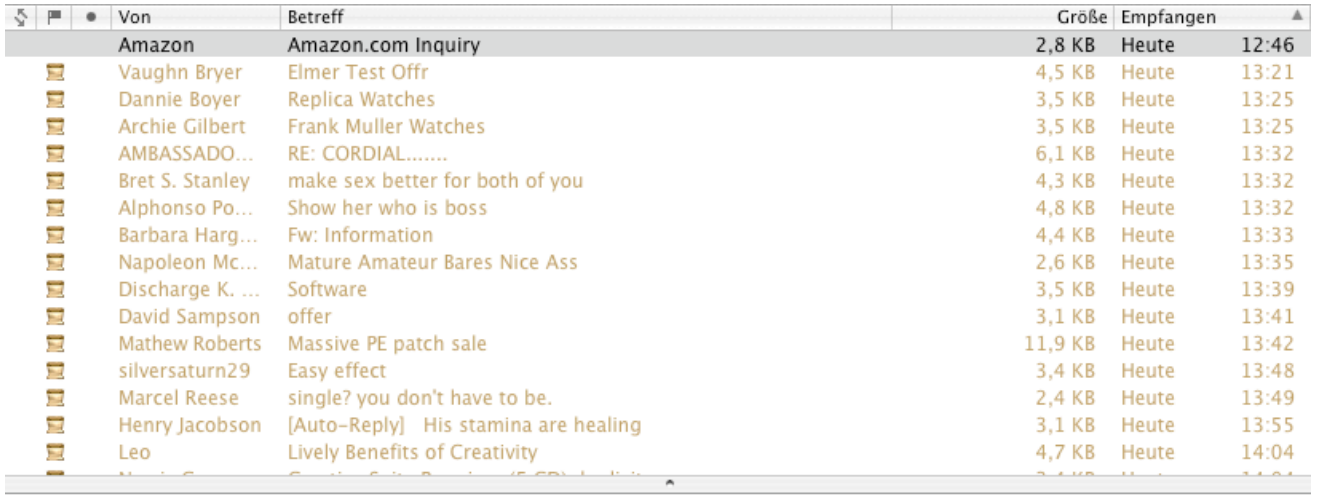
Eigentlich kein Spam

- Viren
- Backscatter
- Mailinglisten
- Phishing

Früher war alles besser

- wenige Spams pro Woche
- bewarben
  - Tintenpatronen
  - Anbieter von Erwachsenenunterhaltung
- Sprache: Englisch
- sofort zu erkennen

Weder Tinte noch Porno



Von	Betreff	Größe	Empfangen
Amazon	Amazon.com Inquiry	2,8 KB	Heute 12:46
Vaughn Bryer	Elmer Test Offr	4,5 KB	Heute 13:21
Dannie Boyer	Replica Watches	3,5 KB	Heute 13:25
Archie Gilbert	Frank Muller Watches	3,5 KB	Heute 13:25
AMBASSADO...	RE: CORDIAL.....	6,1 KB	Heute 13:32
Bret S. Stanley	make sex better for both of you	4,3 KB	Heute 13:32
Alphonso Po...	Show her who is boss	4,8 KB	Heute 13:32
Barbara Harg...	Fw: Information	4,4 KB	Heute 13:33
Napoleon Mc...	Mature Amateur Bares Nice Ass	2,6 KB	Heute 13:35
Discharge K. ...	Software	3,5 KB	Heute 13:39
David Sampson	offer	3,1 KB	Heute 13:41
Mathew Roberts	Massive PE patch sale	11,9 KB	Heute 13:42
silversaturn29	Easy effect	3,4 KB	Heute 13:48
Marcel Reese	single? you don't have to be.	2,4 KB	Heute 13:49
Henry Jacobson	[Auto-Reply] His stamina are healing	3,1 KB	Heute 13:55
Leo	Lively Benefits of Creativity	4,7 KB	Heute 14:04

Von: Amazon <service@amazon.com>
Betreff: **Amazon.com Inquiry**
Datum: 19. November 2005 12:46:06 MEZ
An: Joerg Kinzebach

Dear Amazon member,

Due to concerns we have for the safety and integrity of the Amazon community we have issued this warning.

Per the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Please follow the link below:

http://www.amazon.com.notifications-ssl128.info?/exec/obidos

and update your account information.

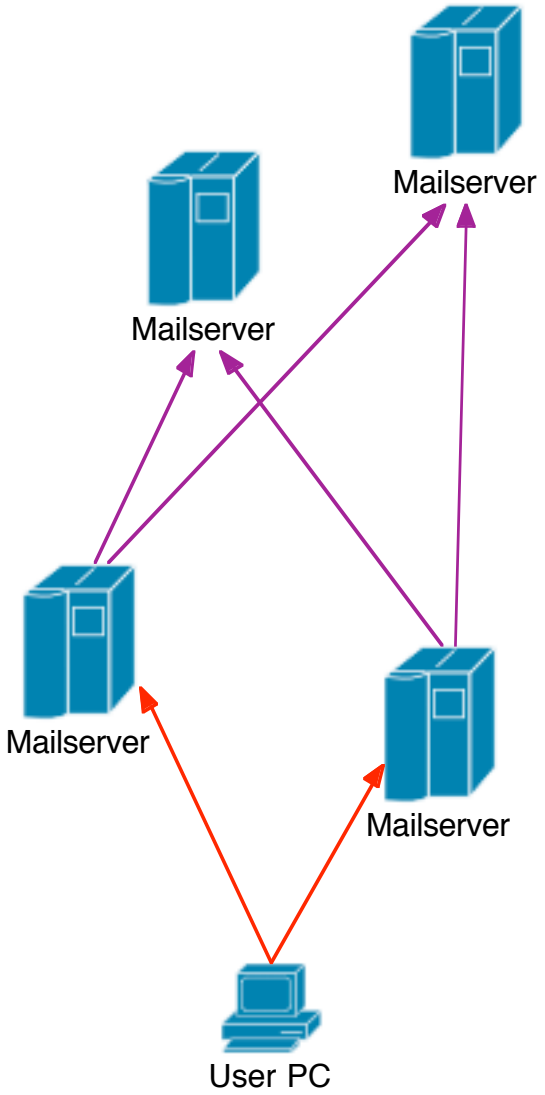
„Antispam“

- Löschen nach Sichtung
- Ende des freien Relayings
- Domain-Tests
- Blacklists
- einfache Filter
- Acknowledged Sender
- Backconnect
- Kombination von Filtern
- Bayes‘sche-Filter
- Razor/DCC
- SMTP-Auth/kein Dialup-Sending
- Greylisting
- SPF
- SenderID
- Domainkeys

Löschen nach Sichtung

- nur bei wenigen empfangen Spam-Mails möglich
- unnötige „Alerts“
- nervenaufreibend

Ende des freien Relaying



- ursprünglich wurde jede Mail von jedem angenommen und ausgeliefert
- Mail-Server hatten keine Konfigurationsmöglichkeit für Limitierung
- nur „externe“ werden ausgesperrt
- anfangs waren ACLs durch Mail-Routing austricksbar (jochen%meier.com@example.com)
- es gibt noch immer und wird auch in Zukunft freie Relays geben

Domain-Test

- Test ob Domain des Senders einer Email existiert
  - Spammer benutzten nie ihren wahren Email-Account sondern nutzten den einfachsten Weg und „erfanden“ Absender-Adressen
  - durch Blocken von erfundenen Domain Namen konnte erfolgreich ein großer Prozentsatz der Spam-Mails abgewehrt werden
- Spammer begannen daraufhin existierende Adressen zu missbrauchen

Blacklists

- meist DNS-basiert
- Beispiele: MAPS, ORBS, spamcop, Dorkslayers
- können systembedingt nur bereits benutze Adressen blocken
- Listen Spam-Sourcen, Open-Proxies, Dialup-IPs, Länder
- Gefahr von veralteten Einträgen
- große Abhängigkeit von Vertrauenswürdigkeit des Betreibers
- Versuch ISPs unter Druck zu setzen
- teilweise absurde Prozeduren für „unlisting“

einfache Filter

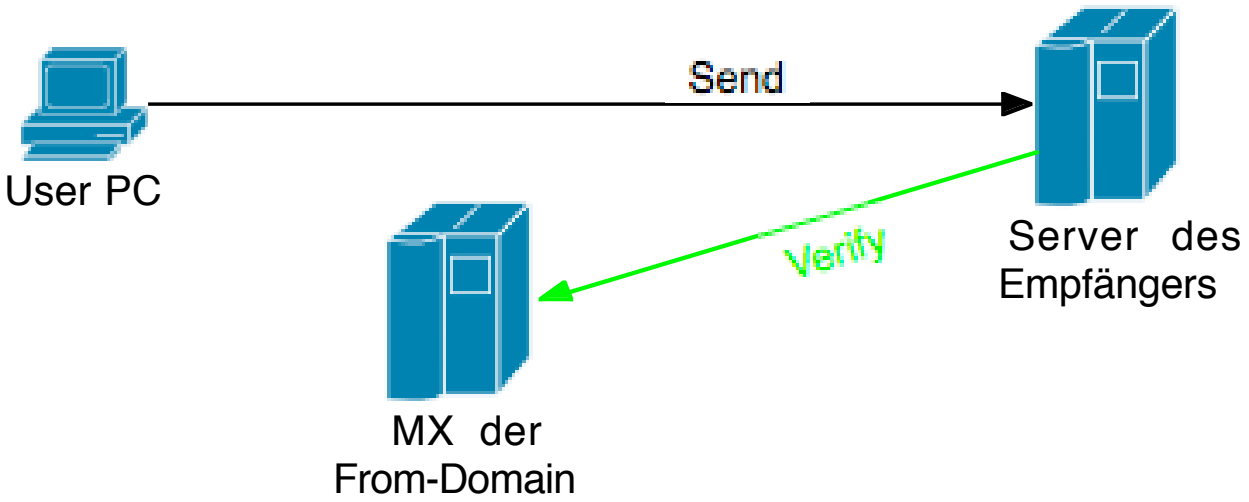
- Simple Regeln, z.B.: „viagra“ im Subject
- Liste der Regeln wächst mit der Zeit ins unermessliche
- leicht zu umgehen („V1a‘Gra“)
- muss für jede neue Art von Spam erweitert werden

Acknowledged Sender

- Absender einer Mail muss eine Kontroll-Mail beantworten um seine Adresse beim Empfänger freizuschalten
- erzeugt zusätzlichen Mailverkehr
- verzögert Mails
- erzeugt bei gefälschten Absendern unerwünschte Mails

Backconnect

- Anfrage bei MX einer Domain, ob Envelope-Sender existiert
- erzeugt zusätzliche Netz- und Server-Last
- „Verify“ Kommando in SMTP eigentlich wegen Spammer abgeschafft



Kombination von Filtern

- Beispiel: SpamAssassin
- vereint viele kleine Filter-Regeln
- Kann durch Bewertung auch Kriterien verwenden, die nicht eindeutig sind
- ist flexibel bei neuen Spam-Formen
- benötigt Updates um geziehltes Umgehen zu verhinden
- nicht sehr anfällig für Ausfälle und/oder DOS

Bayes‘sche-Filter

- statische Berechnung der Spam-Wahrscheinlichkeit Anhand von „Wörtern“
- müssen mit Spam und Ham angelernt werden
- erlauben auch hinreichend gut die Bewertung von neuen Arten von Spam
- Probleme bei weit gestreuten Themengebieten
- Encyclopedia-Content in Mails gegen Bayes Filter

Razor/DCC

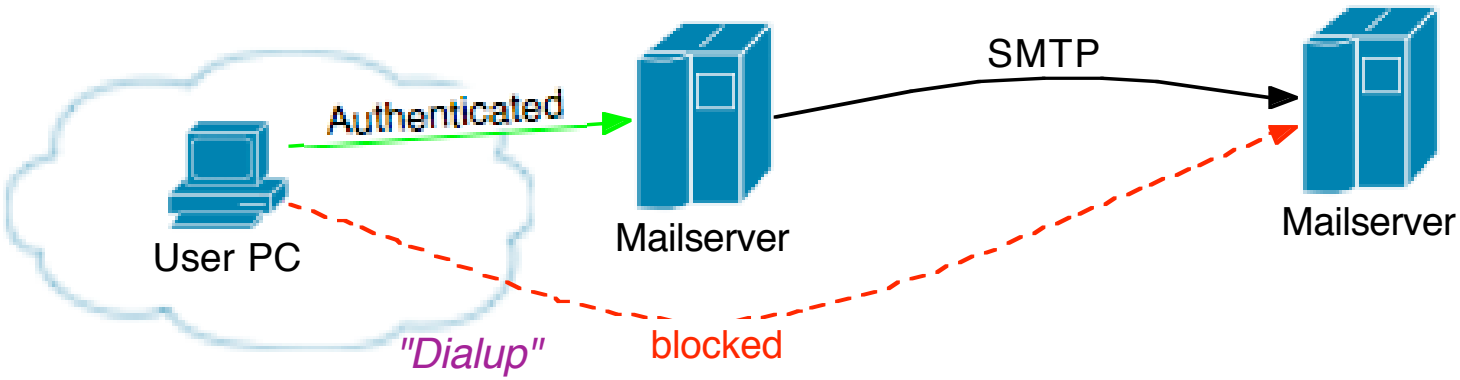
- Bewertung von Nachrichten-Signaturen
- Signaturen werden zentral gehalten
- Razor:
  - Signatur einer Nachricht wird von Nutzern bewertet
  - Nutzer werden anhand ihrer Bewertungen gewichtet
  - Spam-Fallen zur schnellen Bewertung von neuen Spam-Mails
- DCC (Distributed Checksum Clearinghouse)
  - Mails werden anhand ihrer Verbreitung bewertet
  - Erkennt nur bereits weit verbreiteten Spam
  - Keine Spam-Fallen nötig

Computational Testing

- Sender einer Mail muss basierend auf Inhalt aufwendige Berechnungen durchführen
- keine Änderung an Transport
- keine Rückfragen nötig
- keine Updates nötig
- keine Herausforderung für Distributed Computing
- Problem für Mailinglisten

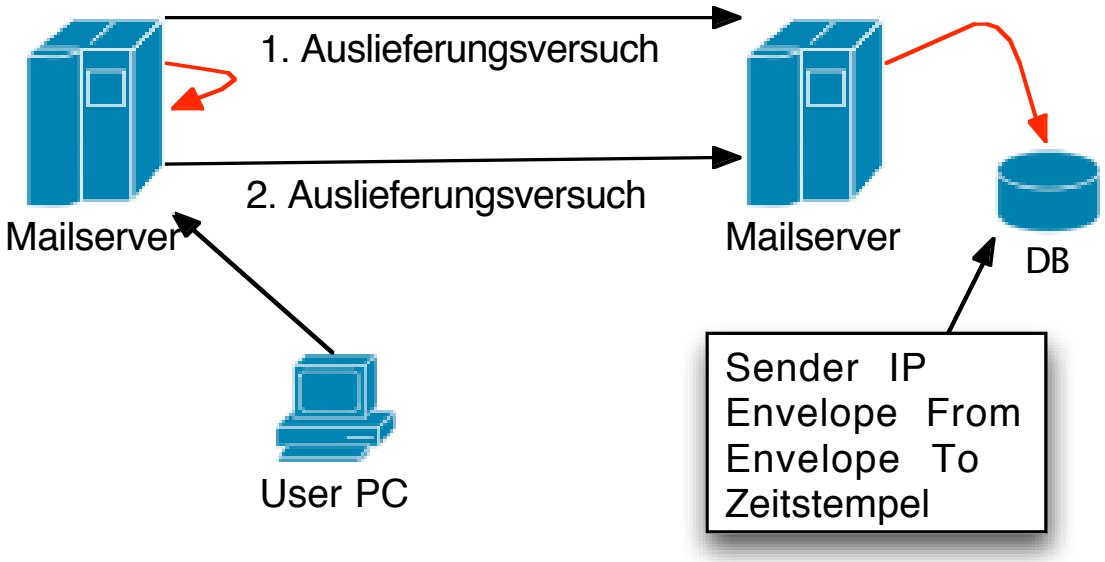
SMTP-Auth/kein Dialup

- Dialup-IPs werden mehr nicht als Quelle für Mails akzeptiert
- Sperrung von Dialup mittles DUL-RBL
- Kein Relaying auf Port 25 (SMTP)
- SMTP nur noch zwischen MTA
- Einlieferung von Nutzer mittels „submit“ (RFC 2476) - erzwingt Authentisierung



Greylisting

- Methode: Vertrauen auf „Retries“
- Spammer versuchen zur Zeit nur einmalige Auslieferung
- mutwilliges Verzögern der Mailauslieferung
- Server-Farmen benötigen „Whitelisting“



SPF

- „Sender Policy Framework“ - Richtlinien für die Verwendung von Domains als Absender in Domains
- Früher: „Sender Permitted From“
- verwendet DNS als „Datenbank“
- durch DNS dezentral verwaltbar ohne zentrale Instanz
- schränkt Missbrauch von Domains zum Spam-Versand ein

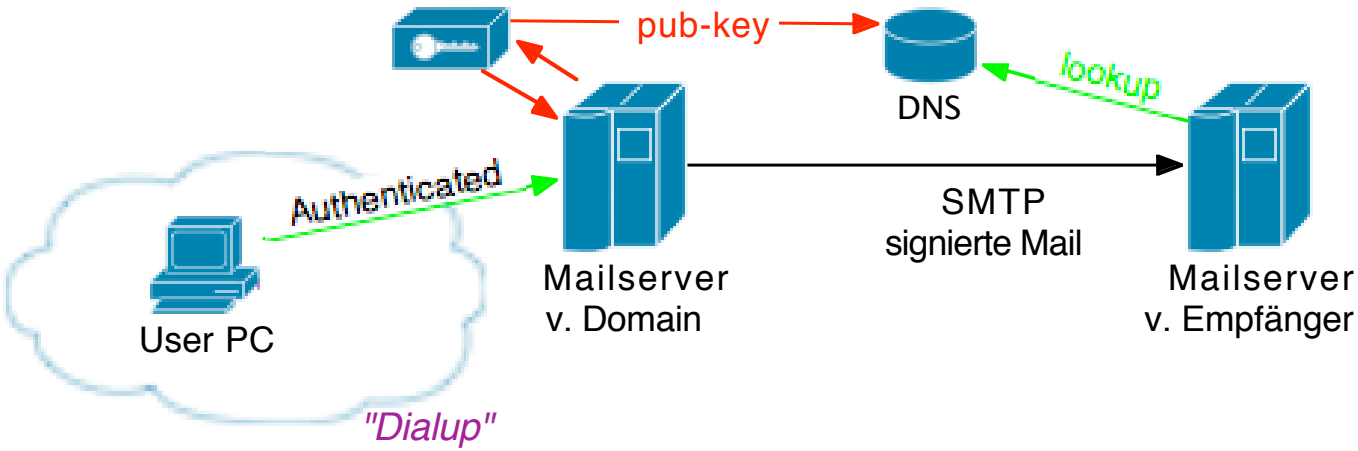
```
> host -t TXT franken.de
franken.de text "v=spf1 mx ip4:193.175.24.0/24
    ip4:193.174.2.0/24 ip4:195.37.132.0/24
    ip4:193.174.159.0/24 ip4:194.94.248.0/24
    ip4:194.94.249.0/24 ip4:193.141.110.0
    ip4:193.174.159.0/24 ip4:194.122.145.0/24 -all"
```

Sender ID

- IETF-Working Group „MARID“ (MTA Authentication Records in DNS)
- Ähnlich wie SPF enthält aber Purported Responsible Address (PRA)
- am 23.09.2004 wurde das Projekt wegen anhaltenden Differenzen innerhalb der Arbeitsgruppe eingestellt
- Microsoft hält Patente an Teilen von „Sender ID“
- Lizenz von Microsoft bzgl. Sender ID würde Verwendung in freier Software verbieten
- Microsoft hält weiter an Sender ID fest

Domain Keys

- authentisiert Absender-Domains
- signiert den Inhalt von Mails
- verhindert unberechtigte Nutzung von Domains und die Manipulation von Mails auf dem Transportweg
- Signierung der Mails mittels RSA
- Mailserver für Signierung verantwortlich



surbl

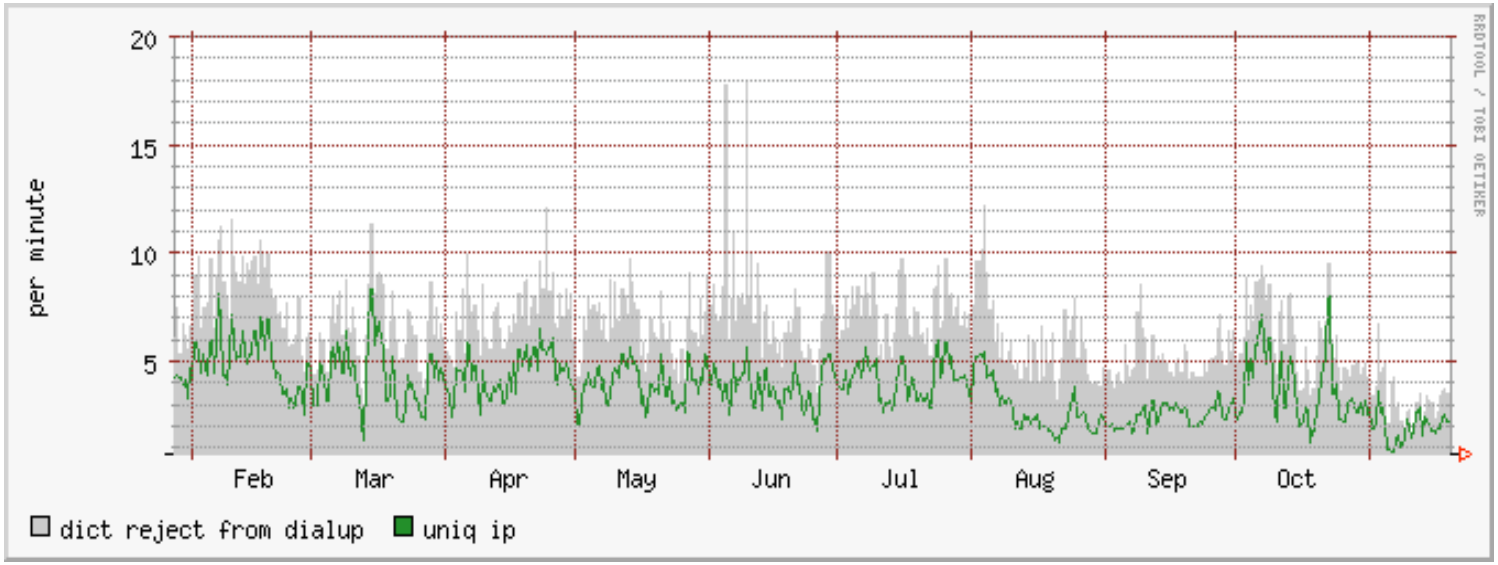
- „Spam URI Realtime Blocklists“
- DNS basierte RBL für URLs
- Spam mit Werbung für Produkte und Dienstleistungen sowie Phishing benötigt Links zu Webseiten
- URLs für beworbene Seiten zu wechseln nicht schnell und häufig möglich
- sehr effektiv und geringes Risiko von False-Positives, da einfaches und relativ fälschungssicheres Kriterium

Opfer von Spam

- Adresse im Usenet „verbrannt“
- Adresse auf Webseiten
- Adresse an CreditCard-Clearinghouse übermittelt
- Adresse erratbar
- In Wörterbüchern von Spam-Virus Opfern

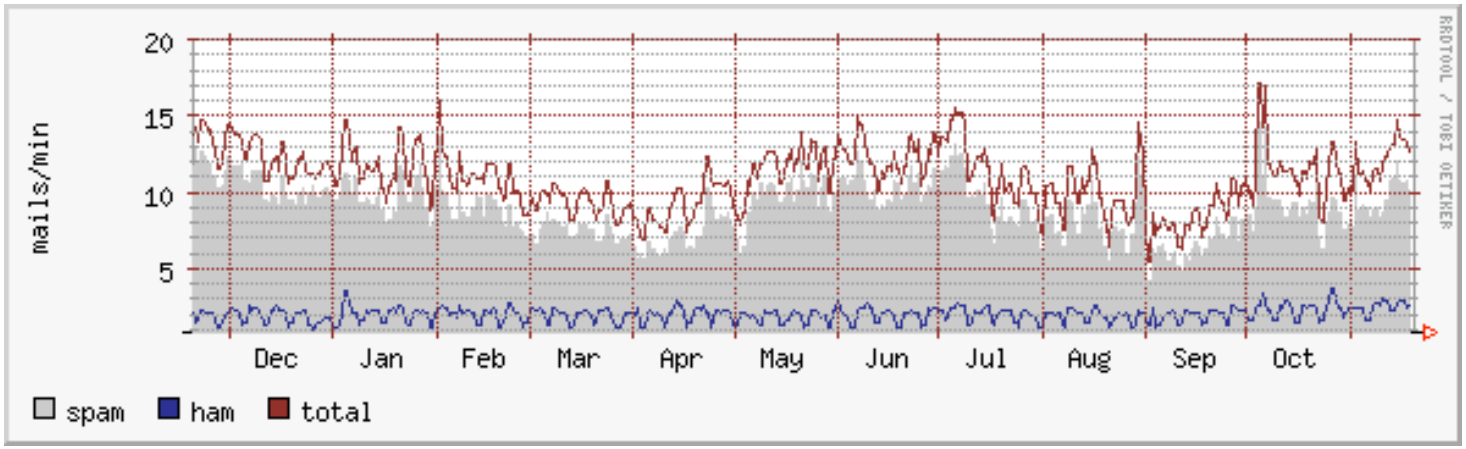
Dictionary-Atacken

- Generierung von Opfer-Adressen durch zusammensetzen von Domain-Namen (öffentlich) und Wörterbüchern für den Nutzer-Part

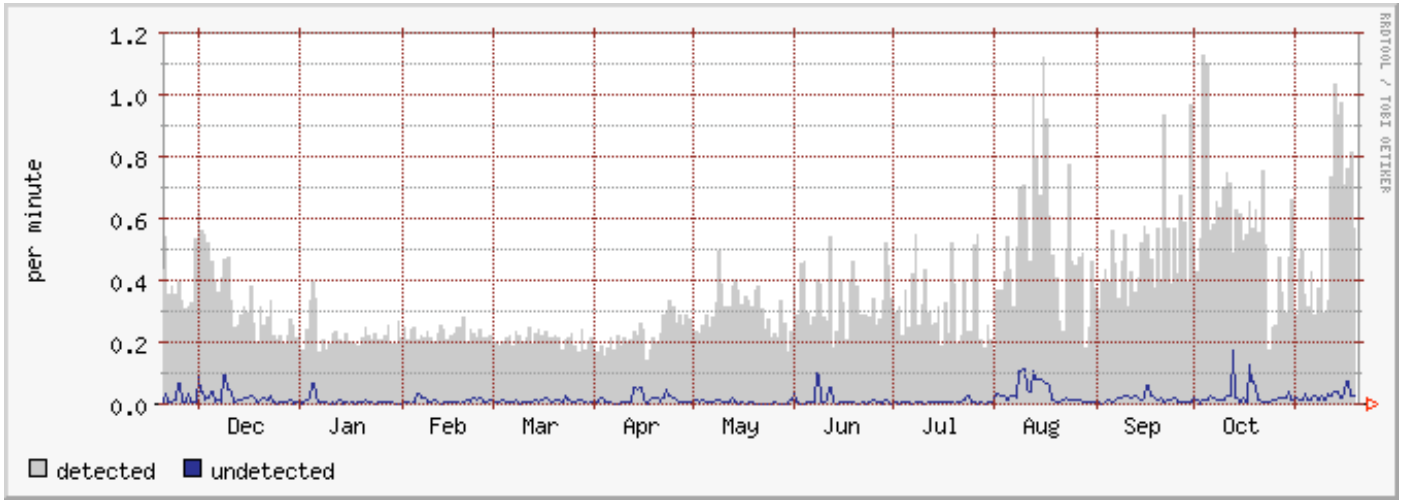


Spam-Entwicklung

- Spam-Tests auf „laurel.franken.de“
- Entwicklung des Mailaufkommens trotz rückläufiger Anzahl von User nicht stagnierend
- auch jahrelang inaktive Adressen sofort nach Freischaltung mit Spam überflutet



KNF-Trap



- 5 Adressen aus 3 Domains
- einmal in alt.test gepostet, sowie auf www.franken.de in Web-Seite versteckt.
- nie zum Versand einer Mail verwendet
- niemals für ein (un-)subscribe benutzt

neue .com Domains 18.11

aaaactiveantiques
aaaadiscountmovers
aaaartists
aaaatravelagency
aaaautofind
aaaautoglassinc
aaabestloan
aaablind
aaablueguide
aaaboobs
aaabridgebank
aaabuildingworld
aaabusinessresources
aaacac
aaacarinsur
aaacarsellerlot
aaacashbackmtg
aaacityrestoration
Aaadiscounters
aaadiscountmerchandise
aaadiscountmtg
aaadiscountshop
aaadreamnow
aaaexoticcars
aaafinearts
aaafloridaticketschool
aaafreedomnow
aaagalleries
aaagameszone
aaagbusiness
aaagenebank
aaaglassonline
aaagse
aaahometheater
aaahotamateurs
aaahotasianamateurs
aaahotlatinaamateurs
aaahouseinspections
Aaahouseinspectors
aaainstantcashmtg
aaaircraft
aaajunkyard
Aaakhmer
aaaleatheritems
aaamarketplace
aaamedswirldwide
aaamedswrldwide
aaamericanautomotive
aaamopids
aaandbenterprises
aaantoniotrading
aaanutzfahrzeuge
aaaoehotel
aaapacstore
aaaplusinc
aaapoolsandspas
aaapromotionsinc
aaaproteomics
aaareadyrooter
aaarealestateschool
Aaaredguide
aaaref

051118 new .com domains : 317759; filesize: 5,1 MB

Links

- DCC: http://www.rhyolite.com/anti-spam/dcc/
- Vipul‘s Razor: http://razor.sourceforge.net/
- Greylisting: http://www.greylisting.org/
- SPF: http://www.openspf.org/
- Sender ID: http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx
- Domainkeys: http://de.antispam.yahoo.com/domainkeys
- SURBL: http://www.surbl.org/