Workshop Spambekämpfung

Linuxwochen 2003

Wien, 5.6.2003

Christian Mock

CoreTEC IT Security Solutions GmbH

<cm@coretec.at>

http://www.coretec.at/spam/workshop.pdf

Inhalt

CoreTEC IT Security Solutions GmbH

- Was ist Spam?
- Wie wird Spam versendet?
- Verschiedene Ansätze zur Bekämpfung
- Erfahrungen mit verschiedenen Techniken
- Wie versende ich Newsletter etc. "sauber"?
- Diskussion

Was ist Spam?

- Begriff kommt aus einem Monty Python-Sketch
- Exaktere Begriffe:
  - "UCE" (unsolicited commercial email)
  - "UBE" (unsolicited bulk email)

Was ist Spam?

- TKG (§101):
  - Die Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken bedarf der vorherigen - jederzeit widerruflichen Zustimmung des Empfängers.
- -> UCE, UBE
- der Punkt ist immer: *unverlangt*

Wie wird Spam versendet?

CoreTEC IT Security Solutions GmbH

- Direkt (vom Sender zum Empfänger), ISPs terminieren oft Account sofort
- dh. Spammer müssen ihre Spuren verstecken, um Account zu behalten
- Gefälschte Header zur Verwirrung
  - Möglichkeit zur automatischen Erkennung
- Absender-Adresse fast immer Fake
  - daher Filtern darauf ziemlich sinnlos

Wie wird Spam versendet?

CoreTEC IT Security Solutions GmbH

- Über "offene Relays"
  - Bei SMTP darf per Design jeder alles
  - Daher bei irgendeinem Server Mails zur Auslieferung zustellen (eine Kopie der Mail, tausende Adressen) und dem die Arbeit und den Stress überlassen

Wie wird Spam versendet?

CoreTEC IT Security Solutions GmbH

- In letzter Zeit sehr viel über offene Proxy-Server
  - http-Proxy bietet neben HTTP- (d.h. Protokollspezifischer) Funktion auch "CONNECT" für TCP-Forwarding (gedacht für HTTPS)
  - CONNECT smtpserver:25 HTTP/1.0
  - keine Spur der originalen Sender-IP-Adresse in der Mail

Ansätze zur Bekämpfung

CoreTEC IT Security Solutions GmbH

- Ablehnen während SMTP
  - technische Charakteristika
  - Blacklisten (lokale und externe)
- Annehmen, dann erkennen, und wegwerfen oder markieren
  - Charakteristika wie oben
  - Zusätzlich inhaltliche Analyse möglich

SMTP: technische Charakteristika

- (Prozentangaben sind % der abgelehnten Verbindungen meines Home-Systems)
- HELO
  - keine Mails ohne HELO annehmen (0%)
  - Syntax-Check auf HELO-String (2,1%)
  - Keine HELOs annehmen, die den eigenen Hostnamen/IP-Adresse enthalten (2,9%)

SMTP: technische Charakteristika

- SMTP Pipelining: nur wenn ausgehandelt (2,2%)
- Domain der Sender-Adresse muß existieren (24%)
- Header/Body auf zb. asiatische Charakter-Sets testen (10.8%)
  (dabei muß die Mail übertragen werden, also weniger Bandbreiten-Ersparnis)

SMTP: technische Charakteristika

- Keine Mail für nicht-existente User annehmen (23,8%)
  (teilweise wird Brute-Force versucht, mögliche Usernamen @irgendeine.domain zu spammen)
- Relaying nicht erlauben (3,4%)
  (sollte bei allen aktuellen MTAs by default inaktiv sein)

Blacklists: lokal

- Keine Mails von IPs aus China, Hongkong, Taiwan, Korea annehmen (4,2%)
  (extreme Maßnahme)
- Diverse ISPs per Reverse-Lookup (5,7%, 5 ISPs)

Blacklists: extern

- "RBL": Real-Time Blackhole Lists
- funktionieren über DNS: z.b. für 209.88.103.4:
- ```
  4.103.88.209.proxies.relays.monkeys.com
   IN A 127.0.0.2
   IN TXT "BLOCKED: See
  http://www.monkeys.com/upl/listed-ip-
  0.cgi?ip=209.88.103.4"
  ```
  ```

Blacklists: extern

- werden aufgrund aller möglicher Kriterien betrieben/befüllt:
  - offene Relays: relays.ordb.org, relays.visi.com
  - offene Proxies: proxies.relays.monkeys.com, opm.blitzed.org, proxy.relays.osirusoft.com
  - Länder, persönliche Vorlieben, ...
- Einschätzung der Qualität tlw schwierig

Blacklists: meine Erfahrungen

- Prozent der gesamt-RBL-Hits:
- proxies.relays.monkeys.com (90%)
- opm.blitzed.org (6,3%)
- relays.ordb.org (3,5%)
- socks.relays.osirusoft.com (0.2%)

Blacklists: mehr Infos

- List of Lists:
  - http://www.declude.com/junkmail/support/ip4r.htm
- Quantitativer Vergleich:
  - http://www.sdsc.edu/~jeff/spam/Blacklists_Compared.html
- Online-Checker für viele RBLs:
  - http://rbls.org/

Content-Analyse

CoreTEC IT Security Solutions GmbH

- IMHO der beste Weg, Spam zu erkennen
- Nachteil: Mail muß übertragen werden
- Kann verschiedenste Eigenschaften einer Mail checken
- Kann anhand der Kombination verschiedener Eigenschaften bessere Entscheidungen treffen als ein simpleres Verfahren

Content-Analyse

- ...am Beispiel SpamAssassin
  - http://www.spamassassin.org
  - Perl, Free Software, Unix/Windows
- Vergibt Plus- und Minus-Punkte
- Summe der Punkte > Schwellwert -> Spam
- dzt. über 800 Tests
- voll konfigurier- und erweiterbar

SpamAssassin

CoreTEC IT Security Solutions GmbH

- Checkt z.B.:
  - Header auf Inkonsistenzen
  - Received-Header gegen RBLs
  - Character-Sets
  - Sprache (heuristische Erkennung)
  - Text-Fragmente
  - MIME-Struktur (Syntax, HTML ohne text/plain, ...)

Bayesische Filter

- Wird mit Beispielen von Spam und Non-Spam gefüttert
- Ermittelt, mit welcher Wahrscheinlichkeit welche Worte vorkommen
- Checkt Mail und errechnet die Wahrscheinlichkeit, daß sie Spam ist

Bayesische Filter

- Idee und erstes Paper von Paul Graham
  - http://www.paulgraham.com/spam.html
- Standalone: bogofilter
  - http://sourceforge.net/projects/bogofilter
- SpamAssassin ab 2.50
- und diverse andere...

Mein Setup...

- Kombination aus allen Techniken
  - SpamAssassin erkennt noch ca. 6% der durchkommenden Mails als Spam
- Kaum False Positives
  - Monitoring aber trotzdem nötig
  - Whitelisting muß möglich sein
- dzt. 0,5-2 Spams pro Tag in der Inbox

Schlechte Erfahrungen...

CoreTEC IT Security Solutions GmbH

- Manche Blacklists
  - ORBS hat nach Gutdünken gelistet
  - Dial-Up-Listen sind gefährlich
- Ignorante Postmaster
  - Mail-Partner eines Kunden auf Open Relay Listen, weil zwar geschlossen, aber nie als geschlossen gemeldet

Schlechte Erfahrungen...

- Filtern auf Hostname-ohne-Domain im HELO
- Filtern auf IPs ohne Reverse Lookup
- Filtern von Received-Headern gegen RBLs
- Generell Setups, die nicht den Bedürfnissen der User angepasst sind

Wie versende ich Newsletter?

CoreTEC IT Security Solutions GmbH

- Problem: wie versende ich legitime Massen-Mails?
- Antwort: Opt-In
  - User muß sich aktiv anmelden
  - Anmeldebestätigung per Mail, sonst Faking möglich
  - Dokumentieren, wann und wie angemeldet
  - keine automatische Anmeldung (vor-selektierte Checkboxen etc)

Wie versende ich Newsletter?

CoreTEC IT Security Solutions GmbH

- Opt-Out ist Böse(tm)!
  - Wenn man sich aktiv **ab**melden muß
  - Widerspricht Netz-Gepflogenheiten
  - Widerspricht dem Gesetz in Ö (Strafe bis 36336 EUR)
  - Wird bei >50% der Österreichischen ISPs zu Problemen führen

Wie versende ich Newsletter?

CoreTEC IT Security Solutions GmbH

- Abmelden bei Opt-In einfach machen
  - Bei jeder Mail im Footer Anleitung...
  - Trotzdem mit manuellem Aufwand rechnen
- Nichts ist unendlich außer der Dummheit
  - daher wird trotzdem irgendwann jemand "Spammer!" schreien

Kurze Werbeeinschaltung

- CoreTEC SMTP Antispam Appliance
  - Sicheres SMTP-Gateway: postfix
  - SpamAssassin
  - auf Kundenwunsch RBLs etc.pp.
  - High Availability
  - Plug In and forget
  - Hard-, Softwarewartung und SpamAssassin-Pflege

http://www.coretec.at/produkte/antispam.html

Danke!

- und eine weiterführende URL zum Abschluß
  http://www.vibe.at/begriffe/