TRALIOS
Linux Server Management

Effektive Möglichkeiten zur SPAM-Bekämpfung

Dipl.-Inform. Dominik Vallendor ▪ 20.08.2012

Über mich

TRALIOS
Linux Server Management

- Dominik Vallendor
- Studium der Informatik in Karlsruhe
- Seit 1995: Internet / E-Mail / Linux
- Seit 2002: Selbständig
- Seit 2010: Tralios IT GmbH: Betrieb von Linux-basierten Web/Mailservern

Überblick

TRALIOS
Linux Server Management

- Das SPAM-Problem
- Tipps für jedermann
- Technische Maßnahmen
- Effektivität
- Fragen & Diskussion

Das SPAM-Problem

TRALIOS
Linux Server Management

- Trotz Twitter & Facebook: E-Mail weiterhin häufigstes Kommunikationsmittel im Internet
- Ca. 95-99% aller E-Mails sind SPAM
- Früher: Versand über offene Relays und gehackte Server
  Heute hauptsächlich: Versand über Botnetze, falsche Absenderkennung
  $\Rightarrow$ Täter nicht zu fassen, Problem dauerhaft

Tipps für jedermann

TRALIOS
Linux Server Management

- Verschiedene E-Mail-Adressen mit eigener Domain nutzen

  Beispiel max+facebook@example.com, max+twitter@example.com, max+2012-08-homepage@example.com

  $\Rightarrow$Adressen lassen sich einzeln sperren / Datenlecks werden identifiziert
- Wg. Backscatter keine Wildcard-Adressen nutzen
- Filterregeln beim Provider bzw. im Mailprogramm nutzen

Technische Maßnahmen I

TRALIOS
Linux Server Management

- Syntaxkontrolle

  Mails abweisen, die von “kaputten“ Mailservern kommen oder Konventionen absichtlich misachten

- Virenfilter

  Automatische Erkennung von Viren/Trojanern anhand von Mustern

- Blacklisten

  Abweisen von Mailservern, über die SPAM versendet wird

  ACHTUNG: Große Unterschiede in der Qualität bei den Spamlisten

  Empfehlung: *NiX-Spam*

  http://www.heise.de/ix/NiX-Spam-DNSBL-und-Blacklist-zum-Download-499634.html

Technische Maßnahmen II

TRALIOS
Linux Server Management

- Greylisting

  Annahme von E-Mails erst nach definierter Wartezeit

  Blockiert einfach gestrickte SPAM-Versender

- Inhaltsbasierte, vordefinierte Filter

  Manuelle Pflege von Listen mit Stichworten, insb. für SPAM-Wellen

- Inhaltsbasierte, dynamische Filter

  Automatische Erkennung von SPAM-Mails anhand von wiederkehrenden Mustern und Begriffen

  Wg. False Positives: Mails nie löschen, nur filtern

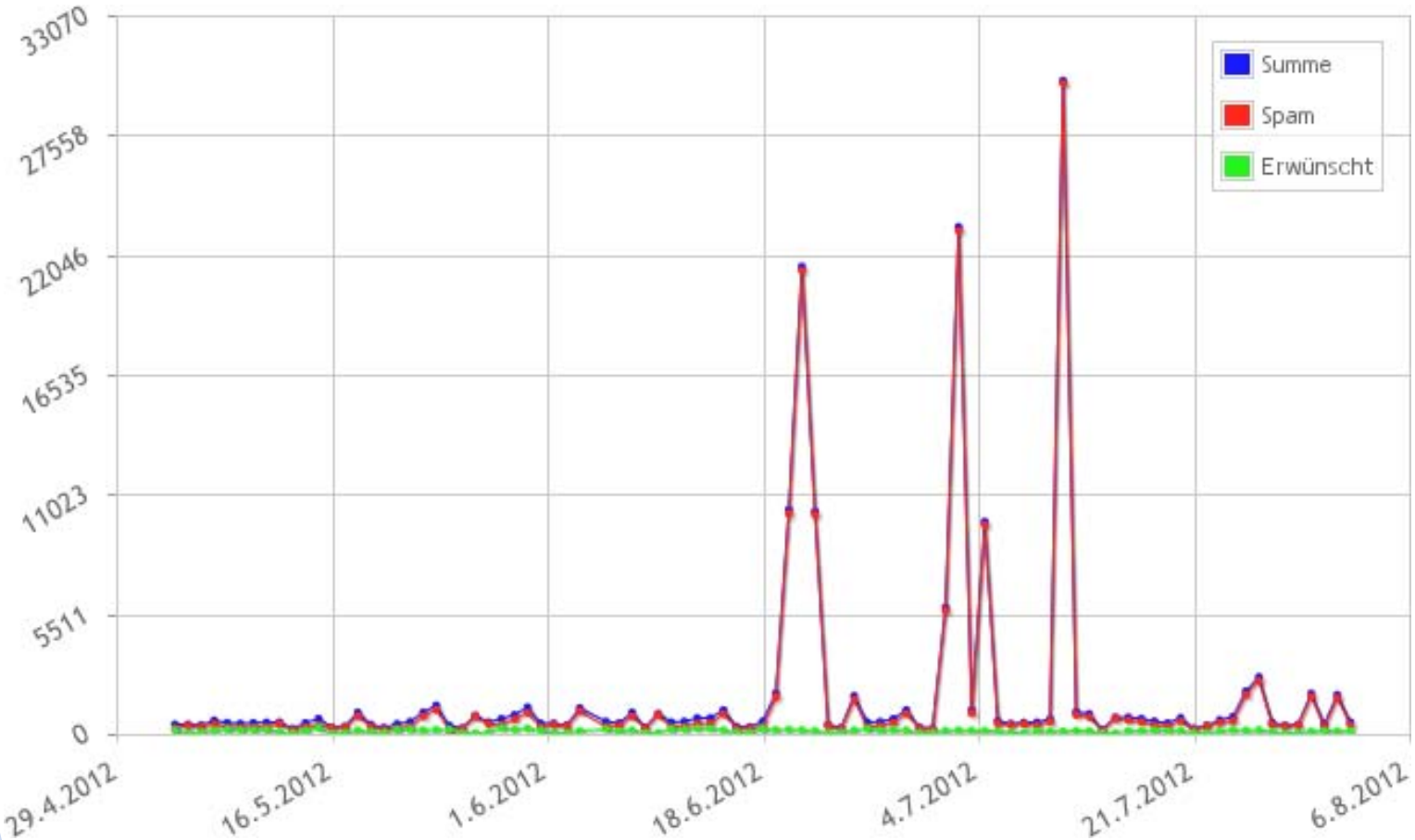
Effektivität

TRALIOS
Linux Server Management

- Abhängig von persönlichem, konsequenten Verhalten
  (Nutzung verschiedener Adressen, manuelle Filter-Pflege)
- Vordefinierte technische Mittel filtern ca. 95% aller SPAM-Mails
- Eigenes SPAM-Filter-Training filtert bis zu 90% vom Rest
- Community-Projekte wie *blackhole.mx* dämmen SPAM-Problem weiter ein
- SPAM-Aufkommen geht bei guten SPAM-Filtern automatisch/dauerhaft zurück

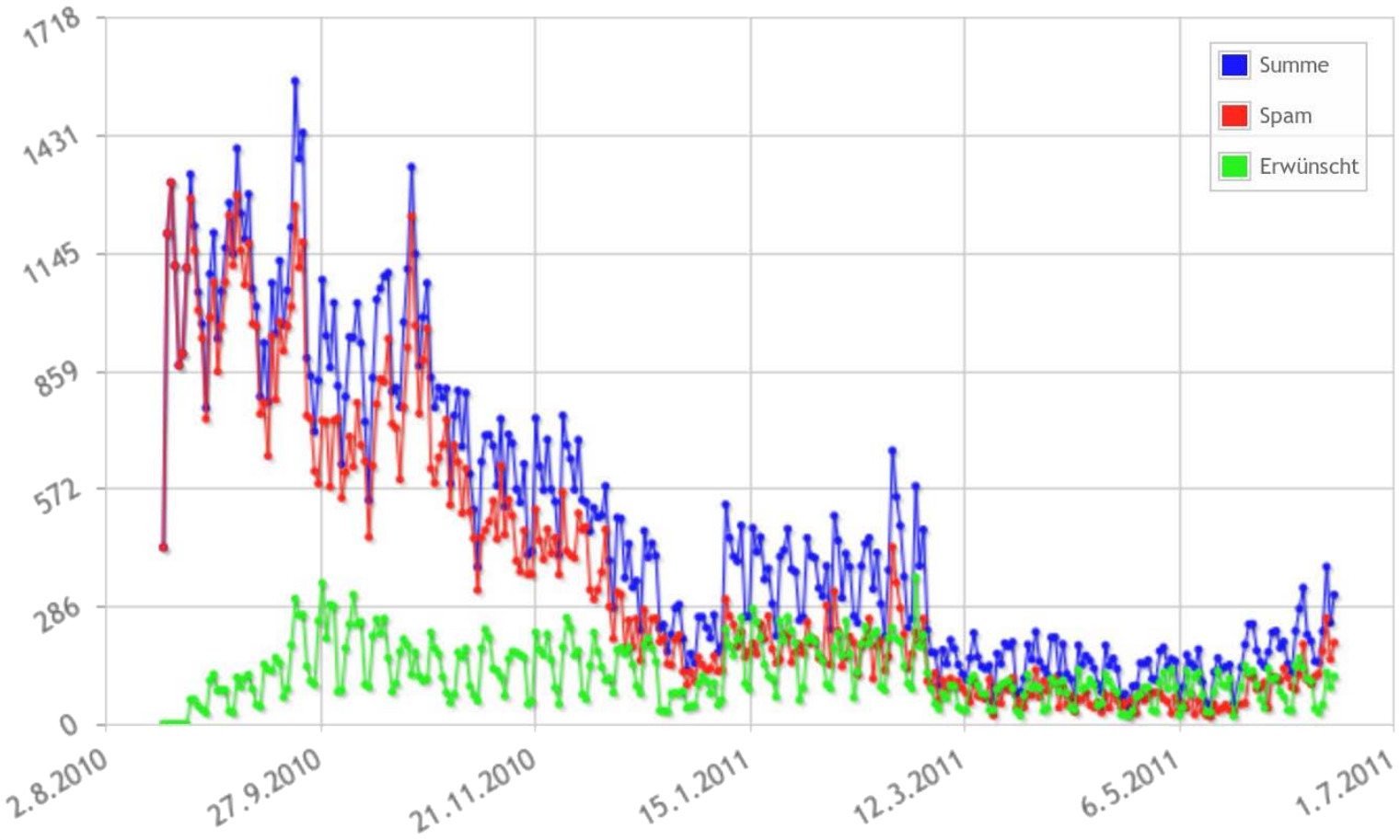
Effektivität

TRALIOS
Linux Server Management



Effektivität

TRALIOS
Linux Server Management



Fazit

TRALIOS
Linux Server Management

- SPAM immer noch großes Problem
- Eigenes Verhalten wichtig
- Durch technische Maßnahmen und Filter-Training lassen sich 99% aller SPAM-Mails blockieren
- Mails immer nur blockieren oder verschieben, nie automatisiert löschen

Fragen & Diskussion

TRALIOS
Linux Server Management

???

Kontakt

TRALIOS
Linux Server Management

- Dipl.-Inform. Dominik Vallendor

- Tralios IT GmbH

  Pfinztalstr. 90

  76227 Karlsruhe

  Telefon: 0721 - 94269660

  Telefax: 0721 - 94269666

  E-Mail/Jabber: vallendor@tralios.de