

Spam mal anders:

Wer sind eigentlich „die Spammer“?

Wie arbeiten Sie?

Wie verdienen Sie?

Und: Aber das kauft doch niemand!

Gleich geht's los...

Geht's um E-Mail....

▶ Peer Heinlein

- ▶ Linux Security Consultant seit 1995
- ▶ Spezialist für Mailserver und Anti-Spam/Anti-Virus
- ▶ Diplom-Jurist / Prädikatsexamen
- ▶ Kunden:
 - ▶ ISPs > 100.000 Kunden (EWEtel, Strato)
 - ▶ Universitäten, Forschungseinrichtungen
 - ▶ diverse Landesrechenzentren (ITDZ, Stuttgart, Baden-Franken, Thüringen)
 - ▶ Div. politische Institutionen und Stiftungen
 - ▶ Spezialfälle >> n-Millionen Mails/Tag (XING, StudiVZ)
- ▶ Heinlein Support GmbH: 17 Mitarbeiter mit Sitz in Berlin

Spam mal anders:

Wer sind eigentlich „die Spammer“?

Wie arbeiten Sie?

Wie verdienen Sie?

Und: Aber das kauft doch niemand!

Spam: Der status quo

In zwei Jahren von heute an ist das Spam-Problem gelöst.

(Bill Gates, Januar 2004, Weltwirtschaftsgipfel in Davos)

- ▶ Ende 2005: 31 Milliarden Spam-Mails pro Tag
- ▶ Ende 2006: 61 Milliarden Spam-Mails pro Tag
- ▶ Ende 2007: 120 Milliarden Spam-Mails pro Tag
- ▶ Ende 2010: 200 Milliarden Spam-Mails pro Tag

200.000.000.000

Spam-Mails pro Tag

73.000.000.000.000

Spam-Mails im Jahr

Wo kommt Spam her: Der Ländervergleich

- ▶ USA 21,3 %
- ▶ Russland 8,3 %
- ▶ China (inkl. Hong Kong) 4,2 %
- ▶ Brasilien 4 %
- ▶ Südkorea 3,9 %
- ▶ Türkei 3,8 %
- ▶ Italien 3,5 %
- ▶ Polen 3,4 %
- ▶ Deutschland 3,2 %
- ▶ Spanien 3,1 %
- ▶ Mexiko 3,1 %
- ▶ Vereinigtes Königreich 2,5
(Quelle: Sophos, Zeitraum Oktober-Dezember 2007)

- ▶ USA 16,4 %
- ▶ Indien 7,3 %
- ▶ Brasilien 5,8%
- ▶ Vereinigtes Königreich 4,3%
- ▶ Südkorea 3,8%
- ▶ Deutschland 3,4%
- ▶ Russland 3,2%
- ▶ Italien 3,1%
- ▶ Vietnam 3,0%
- ▶ Rumänien 2,3%
- ▶ Spanien 2,1%
- ▶ Andere 22,3%
(Quelle: SophosLabs, Report 2010)

Da kommt Spam her: Die Hintermänner

- ▶ IP-Quellen sagen nichts über die Urheber aus
 - ▶ Über 90% des heutigen Spams wird durch Botnetze versandt
- ▶ Wohl aber über:
 - ▶ Anzahl Einwohner eines Landes
 - ▶ Verbreitung von Computern in einem Land
 - ▶ Schutz der jeweiligen PCs
- ▶ Die Urheber des Spam sitzen woanders – oft auch in den USA
 - ▶ Ja, auch in Deutschland.

Wie wird Spam versandt?

882.565

neue Zombie-PCs hat SBL Spamhaus.org
am 24. Juni 2007 entdeckt

(Quelle: spamhaus.org)

36

Sekunden nach der Infektion begannen
die PCs Spam zu versenden.

(Quelle: spamhaus.org)

2.500.000

teilnehmende Zombie-PCs hatte jüngst
das sehr aktive Botnetz „Rustock“

Botnetze und ihr Anteil am weltweiten Spamversand

Rustock

32% - 41%

Grum

23%

Mega-D

17,7%

Webformular-Spam

- ▶ Noch immer sind viele Webformulare nicht gegen Mailversand an Jedermann gesichert
- ▶ Und: Viele Formulare sind nicht gegen Mail-Header-Injection gesichert
 - ▶ Zeilenumbrüche werden aus Header-Feldern nicht herausgefiltert!
 - ▶ Spammer können eigene To:-Zeilen in die generierte Mail einfügen
- ▶ Problem: Webserver relayen über normale Mailserver
 - ▶ Greylisting, Policyd-Weight & Co greifen ausnahmsweise nicht

Bullet-Proof-Server: We will not shut you down!

Adult Bulk Email Hosting

Perfect solution for adult web masters looking for a stable web host for adult oriented email campaigns. This account allows for unlimited traffic.

With our Adult Bulk Friendly Hosting account you get:

- ◆ Unlimited Disk Space
- ◆ Unlimited Monthly Bandwidth
- ◆ We Register and Host Your Own Domain Name
- ◆ 5 POP3 Mailboxes
- ◆ FTP Access to Make Website Edits 24 hours per day
- ◆ Supports PHP4 for Script Support
- ◆ Bullet proof lead or order form script design and implementation
- ◆ 99% Uptime Guarantee
- ◆ We will not shut you down due to complaints
- ◆ Reliable and 100% Bulk Email Friendly!
- ◆ In Business since 1997 - Solid Service - Full Phone Support

The price for this account is:

Monthly \$599 (one time \$20 setup)



Upon receipt of your order, you will receive an email within 24 hours with your FTP access, URL, username, & password.

- ▶ Business Email Hosting:
\$299 / Monat
- ▶ Casino Email Hosting:
\$399 / Monat
- ▶ Adult Email Hosting:
\$599 / Monat
 - ▶ 1 Million Mailadressen:
\$39,95
 - ▶ 98 Millionen Mailadressen:
\$799,95 – special price!
 - ▶ Sitz dieses Angebots:
Fort Lauderdale, USA

Wer sind die Spammer?

Kennt man die Spammer?

- ▶ Viele kennt man sogar
- ▶ Doch man muß sie auch tatsächlich kriegen
- ▶ Und man braucht Gesetze, um sie kriegen zu können











- ▶ Man kennt auch viele Mafia-Bosse...

Wieviele Spammer gibt es?

- ▶ Gar nicht mal so viele.....:
- ▶ 100 namentlich bekannte Spam-Gangs produzieren 80% des Spam-Aufkommens
 - ▶ (Jeweils 1-5 Mitglieder pro Gang)
 - ▶ Quelle: Projekt ROKSO, spamhaus.org

The 10 Worst Spammers

As at 02 February 2011 the world's worst spammers and spam gangs are:

- 1**  **[Canadian Pharmacy](#) - Ukraine**
 A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese web hosting.
- 2**  **[Rove Digital](#) - Estonia**
 Botnets, malware, spam, phishing, DDoS. Inhoster, Cernel, Esthost, Atrivo. What else needs to be said?
- 3**  **[Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov](#) - Ukraine**
 So many Alex & Alexey spamming! Alex Blood tied to Pilot Holding & bbasafehosting.com long ago, then Alex Polyakov posted he owned them. Massive botnet and child-porn spam ring, also pharma, mortgage, and more. May work with Kuvayev and Yambo.
- 4**  **[Vincent Chan / yoric.net](#) - Hong Kong**
 Vincent Chan and his Chinese partners have been sending spam for years. They mainly do pharmacy, and are able to send out huge amounts daily. They use vast numbers of compromised computers -- for sending, hosting and proxy hijacking.
- 5**  **[Peter Severa / Peter Levashov](#) - Russian Federation**
 A spamming partner of Alan Ralsky and other spam gangs.
- 6**  **[Quick Cart Pro](#) - United States**
 American operation with Canadian connections, this large spam operation sells spam-for-hire services using classic "snowshoe" methods with countless IP ranges and domains. Many fictitious identities and aliases.
- 7**  **[Yambo Financials](#) - Ukraine**
 Huge spamhaus tied into distribution and billing for child, animal, and incest-porn, pirated software, and pharmaceuticals. Run their own merchant services (credit-card "collection" sites) set up as a fake "bank."
- 8**  **[Leo Kuvayev / BadCow](#) - Russian Federation**
 Russian/American spammer. Does "OEM CD" pirated software spam, copy-cat pharmaceuticals, porn spam, porn payment collection, etc. Spams using virus-created botnets and seems to be involved in virus distribution. Partnered with Vlad - aka "Mr. Green".
- 9**  **[HerbalKing](#) - India**
 Massive affiliate spam program for snakeoil Body Part Enhancement scams. Also does replica luxury goods, pharma and porn. Spams via botnets, bulletproof hosting offshore and even sometimes uses fast flux hosting.
- 10**  **[Ruslan Ibragimov / send-safe.com](#) - Russian Federation**
 Stealth spamware creator. One of the larger criminal spamming operations around. Runs a CGI mailer on machines in Russia and uses hijacked open proxies and virus infected PCs to flood the world with spam.

SPAMHAUS



Spamhaus

SBL

XBL

PBL

ROKSO

DROP

[Home](#) | [About ROKSO](#) | [ROKSO FAQs](#) | [Advanced Search](#)

Register Of Known Spam Operations



Country: **Russian Federation**

State:

SBL Listings History

[Current SBL Listings](#)

[Archived SBL Listings](#)



Russian/American spammer. Does "OEM CD" pirated software spam, copy-cat pharmaceuticals, porn spam, porn payment collection, etc. Spams using virus-created botnets and seems to be involved in virus distribution. Partnered with Vlad - aka "Mr. Green"

Leo Kuvayev / BadCow

- ▶ [Main Info](#)
- ▶ [Partner-In-Spam: Pavel Kaminski - "Master Splyntr"](#)
- ▶ [Partner-In-Spam: Silmara Barreiros Ferraz](#)
- ▶ [Partner-In-Spam: Vladislav "Vlad" Khokholkov](#)
- ▶ [mailien.net / mailien.org](#)
- ▶ [Another partner or aka: Marshal Mariy](#)
- ▶ [badcow.biz / badcow.org](#)
- ▶ [domain July 2005 \(child porn\)](#)
- ▶ [Domains \(some of the main ones used for DNS, etc.\)](#)
- ▶ [domains August 2005 \(stuffnz.com\)](#)
- ▶ [domains June 2005](#)
- ▶ [domains October 2005 Yesnic \(REGISTRAR-HOLD\)](#)
- ▶ [domains September 2005 Yesnic \(REGISTRAR-HOLD\)](#)
- ▶ [domains September 2005 Yesnic \(REGISTRAR-HOLD\)](#)
- ▶ [Domains \[2005/2006\] \("OEM" pirate warez\)](#)
- ▶ [Domains \[2007\]](#)
- ▶ [Domains \[Jun-2007\]](#)

**Aber mit Spam kann man doch
kein Geld verdienen?**

Aktien-Spam (pump & dump) So wird verdient

- ▶ Aktienkurse kleiner Unternehmen werden manipuliert
 - ▶ Angebliche Geheimtipps werden massiv verbreitet („going to the roof“)
 - ▶ Geringe Nachfragesteigerung löst bei kleinen Aktien große Änderungen aus
 - ▶ Vorher gekaufte Aktien werden lukrativ wieder abgestoßen
- ▶ Ideal anonym nicht-nachvollziehbarer Geldfluß!
- ▶ Trittbrettfahrer wollen ebenfalls profitieren
 - ▶ Sie steigen wissentlich ein

Aktien-Spam (pump & dump)

So wird gehandelt

- ▶ Aktien-Spam-Spammer sind derzeit am erfinderischsten:
 - ▶ GIF-Spam
 - ▶ Interlaced GIF-Spam
 - ▶ PDF-Spam
 - ▶ Word / Excel / ... - Spam
 - ▶ MP3-Spam
- ▶ Ich muß sagen: Hut ab.
 - ▶ Aber: Sie sind zu klug. Ihre eigene Optimierung macht sie schon wieder filterbar...

419 Nigeria-Spam: So wird verdient

- ▶ Einladung zur gemeinsamen Geldwäsche/-abzocke
 - ▶ Millionenerbe verstorbener katholischer Witwen/Priester/Edelmänner
 - ▶ Vertrauen wird durch manuellen Mailwechsel aufgebaut
 - ▶ Geld vom Opfer wird abgezockt
 - ▶ Gleiche Masche wie: „You have won!“
- ▶ Kommt nicht immer aus Nigeria – aber oft :-)
 - ▶ Benannt nach §419 eines nigerianischen Gesetzes (Advance Fee Fraud)
 - ▶ Schwer zu filternder Spam: Wenig charakteristische Merkmale, viel Handarbeit

419 Nigeria-Spam: So wird gehandelt

- ▶ Spammer suggeriert, er müsse dem Opfer vertrauen
 - ▶ Längerer privater manuell geschriebener Mailwechsel
 - ▶ Erzählt private Details, scheint Identität und Motivation offenzulegen
- ▶ Opfer glaubt, die Kontrolle zu haben
 - ▶ Opfer wird vertrauensselig, gibt ggf. auch eigene Daten preis
 - ▶ Opfer macht sich ggf. auch erpressbar

419 Nigeria-Spam: So wird abgezockt

- ▶ Abzocke durch die Sozial-Masche
 - ▶ Auszahlung verzögert sich noch & Spammer gerät in soziale Schieflage
 - ▶ Opfer fürchtet um seine Millionen, bietet soziale Hilfe/Geldspende an
- ▶ Abzocke durch die Vorschuß-Falle
 - ▶ Spammer bittet Opfer, Bankgebühren & Co vorab auszulegen

Porno-/Casino-Spam: So wird gehandelt

- ▶ Wie langweilig: Porno-Webseiten werden beworben.
 - ▶ Gleiches Prinzip bei Online-Casinos
- ▶ Porno-Anbieter spammen nicht – sie lassen spammen
 - ▶ Provision für Werber wird offen angeboten
 - ▶ Spammen ist einkalkuliert, aber den Werbern verboten
- ▶ Eigentlich klassisches Provisionsgeschäft.
 - ▶ Nicht anders: Versicherungen, Verkäufe, Abos...

Porno-/Casino-Spam: So wird verdient

- ▶ Rund 0.01% der Mails können zu billigen Test-Accounts führen
 - ▶ Spammer erhält 30-40% Provision: Ca. 5 Dollar
- ▶ Rund 50% der Test-Accounts werden nicht gleich gekündigt und ziehen mindestens einen Monat Vollaccount nach sich
 - ▶ Spammer erhält 50% Provision: Ca. 20 Dollar
- ▶ Auf 1 Millionen Mails: Ca. 1.500 US-\$
- ▶ Das Kunststück: Viel, aber nicht „zu viel“ Provision generieren
 - ▶ Sonst lohnt es sich für den Betreiber, die Auszahlung der Provision wegen Regelverstoß einzubehalten...

Viagra/Xanax/Cialis/MaleEnhancer-Spam

So wird gehandelt

- ▶ Es geht nichts über den guten alten Online-Shop...
 - ▶ Pro Einkauf winkt die Provision!
- ▶ Aber: Das kauft doch niemand!

Viagra/Xanax/Cialis-Spam

So wird verdient

1.700.000.000

- ▶ 1.7 Milliarden US-\$ betrug der Viagra-Umsatz 2007 bei Pfizer.

346.000.000

- ▶ 346 Millionen US-\$ schaffte Lilly mit Cialis in 2007.

So arbeiten Spammer

So wird Spam anonym versandt

- ▶ Botnetze werden anonym per IRC gesteuert
 - ▶ Command-and-control-Server schwer zu entdecken
- ▶ IP-Netze toter Firmen werden kurzzeitig per BGP wiederbelebt
 - ▶ So gut wie nicht nachvollziehbarer IP-Traffic!
- ▶ Gekaperte Useraccounts zum Spammen innerhalb einer Community
- ▶ Bullet-proof-Server geben Deckung
- ▶ Offene WLANs und anonymes UMTS vereinfachen alles

Immer Probleme mit dem schnöden Mammon

- ▶ Das Problem: Der Geldfluß!
 - ▶ Ein Account pro Zahlung: Paypal & Co
 - ▶ Anonymität im Ausland: Cayman-Islands & Co
 - ▶ Ebenfalls brauchbar: Western Union & Co
 - ▶ Immer wieder gut: Der Scheck zur Einlösung auf dem Nummernkonto
- ▶ Goldene Regel: Gleiche Konten und Zahlungswege nicht mehrfach nutzen. Das Entdeckungsrisiko steigt.

Die Qualität der Mailadressen

- ▶ „Frische“ Mailadressen bringen die besten Klickraten
 - ▶ Neue Nutzer sind unerfahren und naiv
 - ▶ Neue Nutzer sind interessiert an Porno-Angeboten
>15% Klickraten sind möglich
- ▶ Gebrauchte Mailadressen sind oft ihr Geld kaum wert
- ▶ Spammer verkaufen ihre gebrauchten und abgegrasten Mailadressen billig an Einsteiger und andere weiter.

So gelangen Spammer an Mailadressen

- ▶ Einsammeln von Mailadressen im Web
 - ▶ user--AT--domain.de hilft nicht.
- ▶ Finden der Mailadressen auf Privat-PCs per Botnetz
 - ▶ Warum in die Ferne greifen, sieh, das Gute liegt so nah...
- ▶ Offene Foren und Communities
 - ▶ Der Selbstbedienungsladen
- ▶ Gehackte Communities, Mailinglisten, Foren, Firmen-Server
 - ▶ Frischeste und beste Mailadressen!
- ▶ Betreiben von unsubscribe-Portalen
 - ▶ unsubscribenow.org, remove.org, [unsubscribe.net.com](http://unsubscribe.net)

Die Spielverderber: So macht spammen keinen Spaß

Die Gesetzeslage in den USA: CAN-SPAM-Act

- ▶ CAN-SPAM-Act: Anti-Spam-Gesetz seit 2003 in den USA
 - ▶ Verboten ist nicht der unaufgeforderte Versand von E-Mails
 - ▶ Verboten sind irreführende Angaben in Absender & Betreff
- ▶ Kritiker spotten auch: „I-can-spam-act“
- ▶ Aber: CAN-SPAM-Act ermöglicht konkrete Prozesse und hohe Schadenersatzforderungen.
 - ▶ Das bieten deutsches und EU-Recht nicht...

Spammen bedeutet Knast

- ▶ Juni 2006:
Der US-Spammer Daniel Lin zu 3 Jahren Knast verurteilt
 - ▶ Daniel Lin ist damit der erste Spammer, den der CAN-SPAM-Act trifft
 - ▶ Außerdem 10.000 US-\$ Geldstrafe
 - ▶ Er hatte für Potenzmittel und Kräuterpillen geworben und sich schuldig bekannt
- ▶ Oktober 2007:
Zwei Spammer werden in den USA zu 5 Jahren Knast verurteilt
 - ▶ 2 Millionen Porno-Werbemails wurden konkret nachgewiesen
 - ▶ Sie verdienten in vier Jahren angebl. rund 2 Millionen Dollar.
- ▶ Noch offen: Jeremy Jaynes zu 9 Jahren Knast verurteilt
 - ▶ Während der Berufung gegen eine Kautions von 1 Million US-\$ auf freiem Fuß
 - ▶ März 2009 freigesprochen weil Anti-Spam-Gesetz verfassungswidrig war

Spammen ist gefährlich...


- ▶ Vardan Vardanovich Kushnir wurde am 24. Juli 2005 brutal erschlagen in seiner Wohnung aufgefunden
 - ▶ Er hatte massiv Spam-Werbung für Sprachkurse gemacht
 - ▶ 2003/2004 erreichte er bis zu 25 Millionen Empfänger
- ▶ Sein Problem: Er wählte Russen als Zielgruppe
 - ▶ Die Kripo stellte später jedoch eine Tötung in Selbstverteidigung fest, als er sich drei Damen anzüglich nähern wollte. Ein Zusammenhang zum Spammen wurde verneint.

Spammen kann teuer werden...

- ▶ James McCalla wurde verurteilt
 - ▶ Der Spammer aus Florida hatte 280 Millionen Spam-Mails ausgesandt
 - ▶ Als Absender hatte er den Provider cis.net gefaked
 - ▶ Er wurde deshalb nach dem CAN-SPAM-Act verurteilt
- ▶ Das Urteil: Schlappe 11.2 Milliarden US-\$ Schadenersatz
 - ▶ Viel schlimmer: Nun darf er drei Jahre lang das Internet nicht nutzen.



**Darum:
Bleibt sauber (im doppelten Sinne).**



Heinein - Professional Linux Support GmbH - Heinein Support - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.heinein-support.de/web/heinein/index/

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

**AKADEMIE
SUPPORT
HOSTING**

Heinein Support
News
Fact Paper
Referenzen
Jobs bei uns
Fachbücher unseres Teams
Unsere Vorträge zum Download
PCdenzfall - Der Micosoft-Blues
Impressum
Kontakt

Suche

Fertig

Fachkompetenz.
Täglich auf unserer CeBIT-Bühne in Halle 6 Stand G 41.

CeBIT **Linux höchstpersönlich.**
Unsere Erfahrung ist Ihre Sicherheit.

CeBIT 2009
Diese Jahr werden wir erstmals auf unserer eigenen CeBIT-Bühne zahlreiche Fachvorträge für Sie präsentieren.
[weiterlesen ...](#)

4. Mailserver-Konferenz
Die Vorbereitungen für die 4. Mailserverkonferenz in Berlin sind in vollem Gange. Postmaster und Administratoren, die über die aktuellen Entwicklungen auf dem laufenden bleiben wollen können sich jetzt schon für ihr Wissens-Update anmelden.
[weiterlesen ...](#)

Persönlich und direkt – von Profi zu Profi.
Linux-Kompetenz auf höchstem Niveau, direkt und frei von Attitüden. So einfach lässt sich beschreiben was wir bieten. Jeder von uns ist hochspezialisiert auf seinem Gebiet, besitzt langjährige Erfahrung und ist international "Linux Professional Institute Certified" (LPIC-1, LPIC-2). Mit fundierten Linux-Lösungen aus der Praxis haben wir uns einen Namen gemacht und geben dieses Wissen gerne weiter: in Büchern, Fachzeitschriften und auf Kongressen, an unserer Akademie und im individuellen Support.

Heinein Akademie
Wir kennen das "who is who" der Linux-Profis und engagieren für jedes Thema den optimalen Dozenten. Das ist die Heinein Akademie: Unsere Teilnehmer erhalten das Linux-Know-How erstklassiger Referenten in

Referenzkunden
Ärzte ohne Grenzen
ARD Stern Kommunikationsnetze
AMD Saxony

Ja, diese Folien stehen als PDF im Netz...
<http://www.heinein-support.de>

Soweit, sogut.

Fragen? Fragen!

Dann:

**Bis hierhin vielen Dank,
bis nachher.**