HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Spam mal anders:

Wer sind eigentlich „die Spammer“?
Wie arbeiten Sie?
Wie verdienen Sie?
Und: Aber das kauft doch niemand!

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Spam:
Der status quo

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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 2008: Prognostizierter Anstieg von +40% lt. Ironport

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

120.000.000.000

Spam-Mails pro Tag

43.800.000.000.000

Spam-Mails im Jahr

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Wo kommt Spam her: Der Ländervergleich

- USA 23,2 %
- China (inkl. Hong Kong) 20,0 %
- Südkorea 7,5 %
- Frankreich 5,2 %
- Spanien 4,8 %
- Polen 3,6 %
- Brasilien 3,1 %
- Italien 3,0 % (Neueinsteiger)
- Deutschland 2,5 %
- Großbritannien 1,8 %
- Taiwan 1,7 %
- Japan 1,6 %

(Quelle: Sophos, Zeitraum April-Juni 2006)

- 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)

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Wie wird Spam versandt?

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

882.565

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

(Quelle: spamhaus.org)

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

36

Sekunden nach der Infektion begannen die PCs Spam zu versenden.

(Quelle: spamhaus.org)

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

1.800.000

teilnehmende Zombie-PCs hat das derzeit größe Botnetz „Storm Worm“

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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)

Order Now

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

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Wer sind die Spammer?

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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...

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

The 10 Worst ROKSO Spammers

As at 28 February 2008

Rank	Photo	Spammer or Spam Gang	Country
1		**Leo Kuvayev / BadCow** 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"	**Russian Federation**
2		**Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov** 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.	**Ukraine**
3		**Vincent Chan / yoric.net** 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. The use a vast amount of compromised machines, for sending, hosting and proxyhijacking.	**Hong Kong**
4		**Russian Business Network** Among the world's worst spammer, child-pornography, malware, phishing and cybercrime hosting networks. Provides "bulletproof hosting", but is probably involved in the crime too.	**Russian Federation**
5		**Nikhil Kumar Pragji / Dark-Mailer** Through the Dark-Mailer Windows based proxy-botnet based spamware, this spammer is responsible for and behind a large portion of the world's illegally send spam.	**Australia** Queensland
6		**Ruslan Ibragimov / send-safe.com** 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.	**Russia**
7		**Pavka / Artofit** A Russian gang who have been spamming for years. Started with porn, now into many types of spam, always via hijacked PCs. Part of a large criminal group involving ROKSO spammers Leo Kuvayev & Alex Blood. Also see "Yambo Financials" ROKSO.	**Russia**
8		**HerbalKing** Massive affilitiate 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.	**India**
9		**Yambo Financials** 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."	**Ukraine**
10		**Michael Lindsay / iMedia Networks** Lindsay's iMedia Networks is a full-fledged spam-hosting operation serving bulletproof hosting at high premiums to well known ROKSO-listed spammers. His customers spam via botnet zombies with spam payloads hosted offshore, tunneled back to his servers.	**United States** California

Source: Register Of Known Spam Operations (ROKSO) database + Spamhaus Blocklist (SBL) database. Detailed records on each spammer or spam gang listed can be viewed by clicking on the hyperlinks above.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SPAMHAUS

THE SPAMHAUS PROJECT

Spamhaus | SBL | XBL | PBL | ROKSO | DROP

Home | About ROKSO | ROKSO FAQs | Advanced Search

Register Of Known Spam Operations

Search

ROKSO

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]

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Aber mit Spam kann man doch kein Geld verdienen?

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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...

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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 vertrauensseelig, gibt ggf. auch eigene Daten preis
  - Opfer macht sich ggf. auch erpressbar

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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...

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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...

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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!

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

So arbeiten Spammer

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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, unsubscribenet.com

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Die Spielverderber: So macht spammen keinen Spaß

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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...

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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 James zu 9 Jahren Knast verurteilt
  - Das Urteil geht durch mehrere Berufunsinstanzen und ist noch offen
  - James ist derzeit gegen eine Kaution von 1 Million US-$ auf freiem Fuß

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

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.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

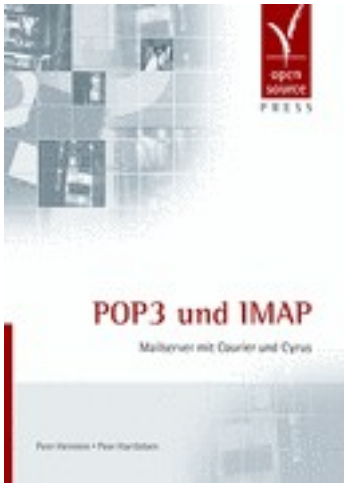
Darum:

Bleibt sauber (im doppelten Sinne).

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Wenn es um echtes Papier geht:

- „POP3 und IMAP“
  Mailserver mit Courier und Cyrus
  - Erläutert auch Detailwissen über IMAP und Mailstorage
  - Courier sehr einfach auf Dovecot übertragbar,
    Prinzipien und nötiges Wissen sind identisch



- Das Postfix-Buch
  Sichere Mailserver mit Postfix
  - Der Klassiker mit rund 750 Seiten
  - Deckt auch Anbindung der IMAP-Server ab
  - Ab ca. Juni 2008 in stark überarbeiteter 3. Auflage

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Heinlein Support hilft auch bei allen Fragen rund um E-Mails:

- AKADEMIE
  - Von Profis für Profis: Wir vermitteln die oberen 10% Wissen. Geballtes Wissen und umfangreiche Praxiserfahrung aus erster Hand.
- SUPPORT
  - Wir sind das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im Heinlein CompetenceCall Notfälle, auf Wunsch auch in SLAs mit 24/7-Verfügbarkeiten.
- HOSTING
  - Wenn Hosting kein Massengeschäft sein darf: Individuelles Business-Hosting mit perfekter Maintenance durch unsere Linux-Profis. Sicherheit und Verfügbarkeit werden bei uns groß geschrieben.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Und nun...

- **Vielen Dank für's Zuhören...**
- **Schönen Nachmittag noch...**
- **Und viel Spaß an der Tastatur.**
- **Bis bald.**

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Heinlein Support hilft auch bei allen Fragen rund um E-Mails:

- AKADEMIE
  - Von Profis für Profis: Wir vermitteln die oberen 10% Wissen. Geballtes Wissen und umfangreiche Praxiserfahrung aus erster Hand.
- SUPPORT
  - Wir sind das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im Heinlein CompetenceCall Notfälle, auf Wunsch auch in SLAs mit 24/7-Verfügbarkeiten.
- HOSTING
  - Wenn Hosting kein Massengeschäft sein darf: Individuelles Business-Hosting mit perfekter Maintenance durch unsere Linux-Profis. Sicherheit und Verfügbarkeit werden bei uns groß geschrieben.