The Art of Spam

Vergangenheit, Zukunft, Technik

Jörg Kinzebach <joerg@duck.franken.de>

Happy Birthday

- Spam wurde 30 Jahre alt
- Gesendet am 3. Mai 1978 eines DEC Vertriebsmitarbeiters an alle Nutzer des Arpanet um eine Marketing-Präsentation für das neue Dec-20 System zu bewerben

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE
DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE
DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM
AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T
AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM.
THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040
AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE
DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER
DECSYSTEM-20 MODELS.

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY
AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS
MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM
HYATT HOUSE (NEAR THE L.A. AIRPORT)
LOS ANGELES, CA

THURSDAY, MAY 11, 1978 - 2 PM
DUNFEY'S ROYAL COACH
SAN MATEO, CA
(4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER
DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND,
PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE
FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY.

Spam

Vergangenheit und Gegenwart

Spam damals

- Bewerben von Produkten
- Einfache Gestaltung des Spams, oft sehr direkte Produktwerbung
- Spammer war identisch mit Produkterzeuger/-vertrieb
- Sehr viel Handarbeit in der Verbreitung des Spam und der Pflege der Empfängerliste

Bill Gates

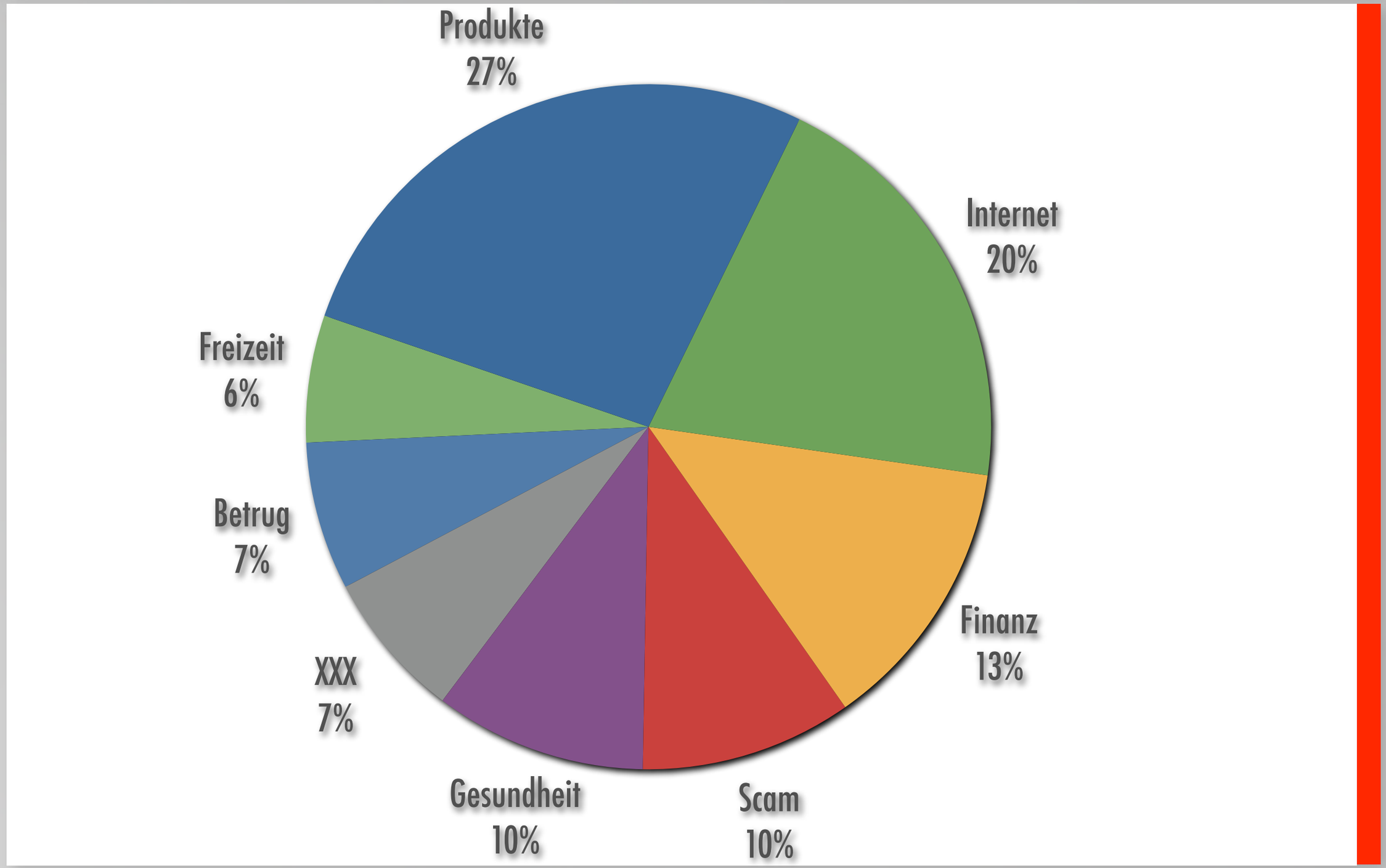
- DAVOS, 24. Januar, 2004 vor den Teilnehmern des Weltwirtschaftsforums:

"Two years from now, spam will be solved"

Spam heute

- Kaum noch Übereinstimmung von Werber und Beworbenem
- Spam wird kaum noch von Systemen des Spammers versendet
- Keine Handarbeit sondern spezialisierte Software
- Spam als Hilfsmittel für Betrug
- Adresssammlung, System-Pflege, Softwareentwicklung und Spam-Betrieb durch Arbeitsteilung professionalisiert
- Aggressive Verbreitungsstrategien, die auch die Überlastung der Empfänger in Kauf nehmen
- Spam und Spambekämpfung im Kriegszustand

Spam Typen



PDF-Spam

- Verstecken des Spams vor Filtern
  - kein durch Text-Scanner direkt untersuchbarer Inhalt
  - leicht diversifizierbare Signaturen des Spams um Hash-Datenbanken zu umgehen
  - grafische Gestaltungsmöglichkeiten des Inhalts
- "teurer" zu analysieren als Text oder Bilder
- Infizierung des Empfänger-Rechners
  - "PDF Worm" aka "Peachy", "Adobe Acrobat Worm"
  - "W32/AdobeReader.K", "Exploit.Win32.PDF-URI.K"
- Löste Image-Spam ab
- Trend stark rückläufig seitdem Filter auch PDFs untersuchten können

Web-Spam

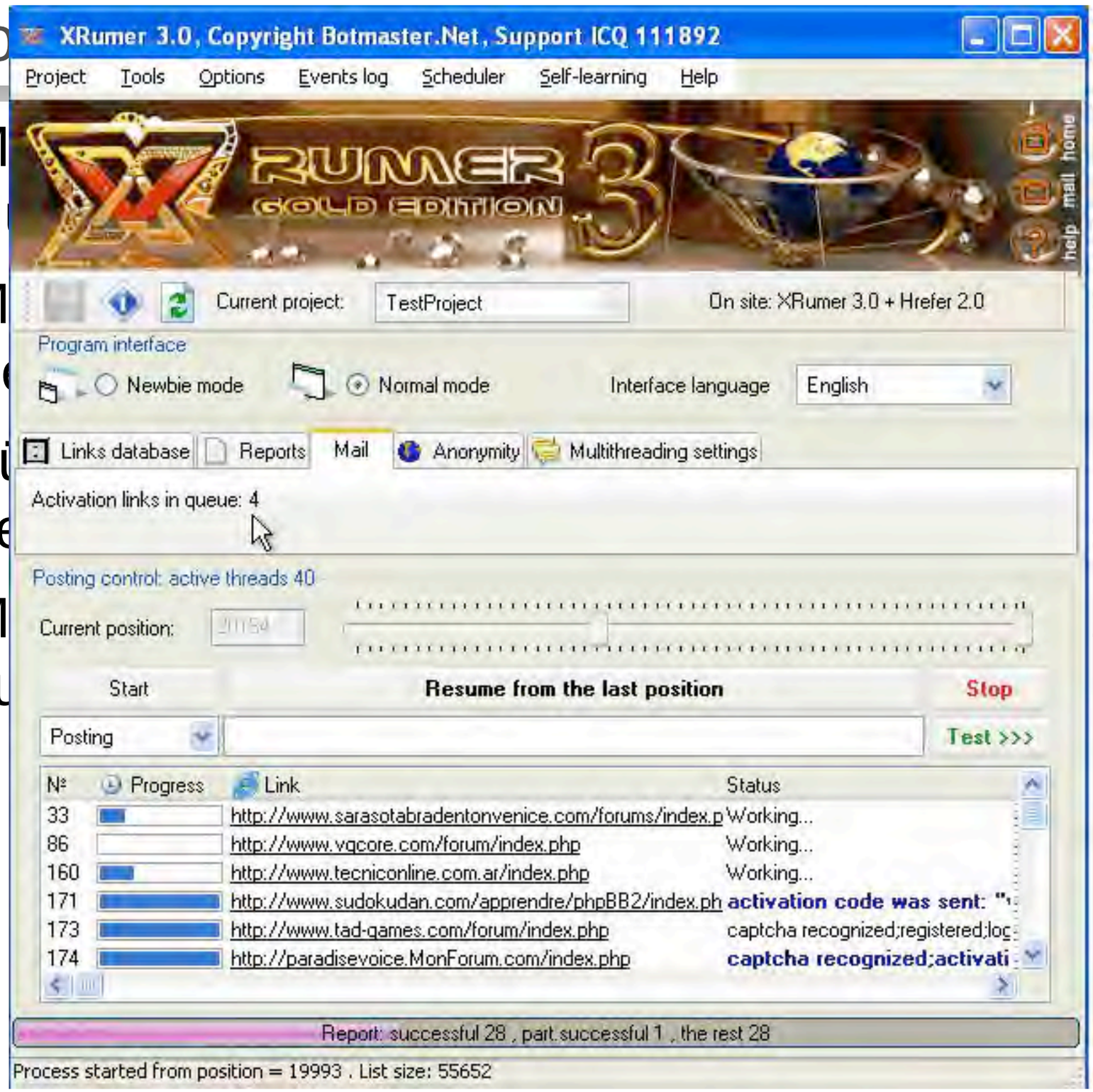
- Web-Seiten, die aufgrund ihrer Beschaffenheit Nutzer auf sich ziehen
  - Content-Spam
    - Künstlicher Inhalt enthält sehr viele Suchbegriffe
    - Inhalt wird von echten Seiten "entliehen" und "erweitert"
  - Link-Spam
    - Seiten verlinken zu immer weiteren Seiten um den "Link-Count" zu erhöhen und somit in Suchmaschinen besser bewertet zu werden
    - "Link-Tausch" mit Partner-Seiten
    - Links in fremdem Content erstellen(Gästebücher, Foren usw.)

Web-Spam

- Einblendung von Werbebannern
- Nutzer zu eigenen Inhalten führen
  - Vortäuschen weiterer interessanter Informationen (Nutzer-Interaktion)
  - Automatisierte Weiterleitung
- Phishing
  - Viele Nutzer verwalten keine Bookmarks sondern "suchen" sich Seiten immer wieder
  - "Zufällige" Weiterleitung auf Dienst, für den man Anmeldedaten besitzt

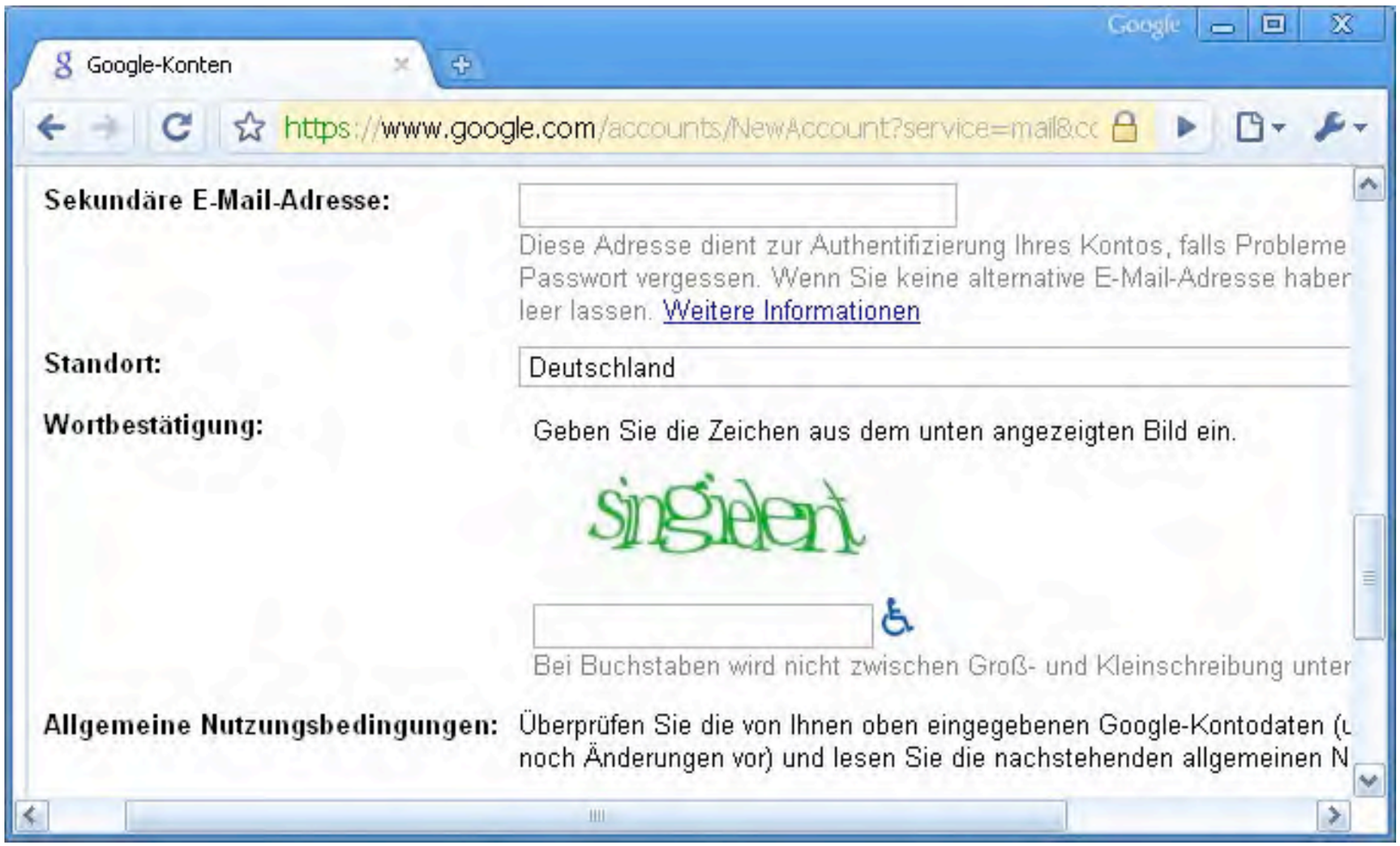
Fo

- M… …iven N…
- M… …ann B…
- Fi… …erden "on-de… …egistriert
- M… …ungs-Link zu…



Captcha

- Abwehr von Robots
- Menschliche Besucher sollen eine Aufgabe meistern um zu beweisen, dass sie kein Bot sind

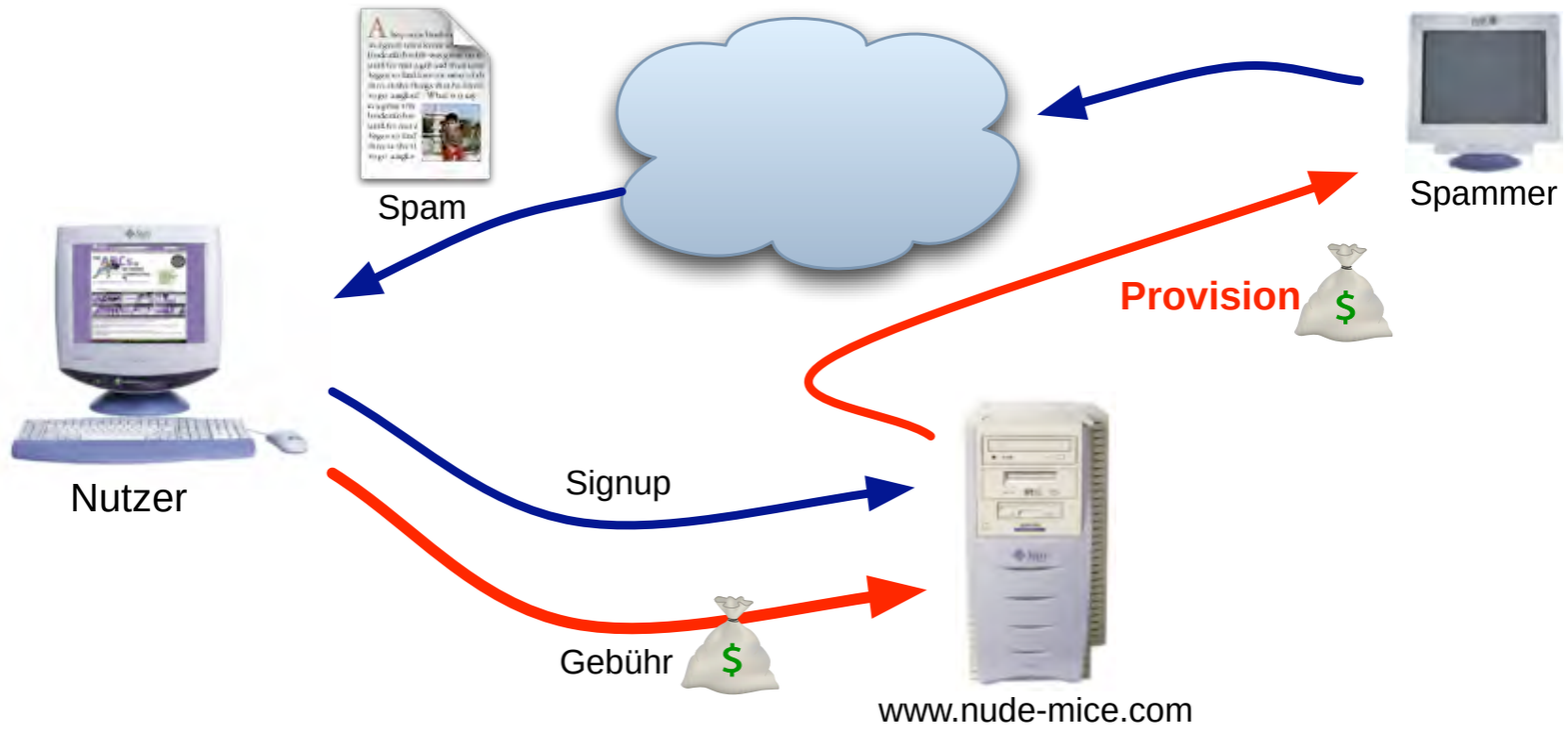


Captcha-Spam

- Sowohl durch Spam beworbene Web-Site als auch durch Spam verbreitete Malware fordert Nutzer dazu auf, Captchas zu lösen um an "Prämium-Inhalte" zu gelangen
- In Wirklichkeit werden Captchas anderer gelöst, damit der Spammer Zugriff zu Ressourcen erhält

Affiliate Spam

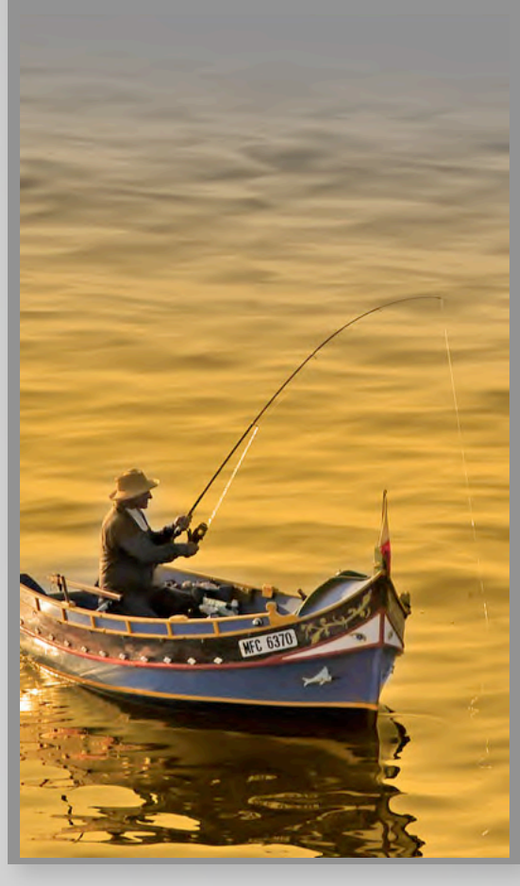
- Provision durch Vermarktung von Diensten anderer
- Beispiel für Affiliate Programme:
  - Webmaster-Programme vor allem im Bereich der "Erwachsenenunterhaltung"
  - Amazon
- Banner



Affiliate Spam

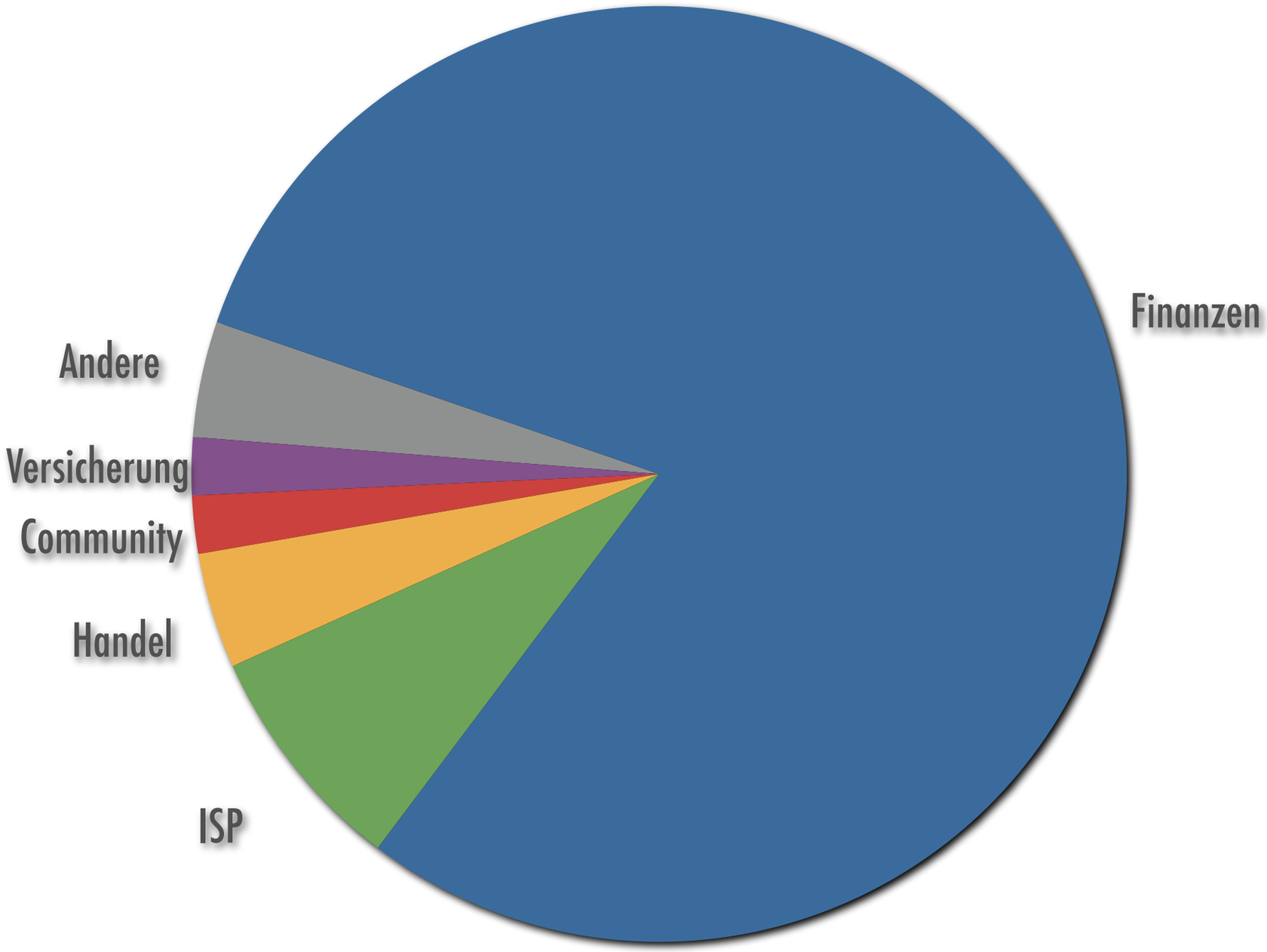
- Werbepartner mittels Web-Formular
- Oftmals sehr unrestriktive Geschäftsbedingungen
- Sehr schwer verfolgbare Geschäftsbeziehungen
- Produkt- bzw. Dienstanbieter nicht direkt verantwortlich für Werbung durch Affiliate-Partner
- Einzelner Affiliate kann im Zweifelsfall als das schwarze Schaf herausgestellt werden

Phishing



- Nutzer werden durch Tricks dazu gebracht vertrauliche Daten an den Angreifer zu übermitteln
  - Bankkonto/Visakarten-Daten
  - Account-Namen und -Passwörter
  - Name, Adresse und Geburtsdatum
- Verschiedenste Methoden
  - Links zu Phising-Website
  - Gefälschte E-Mails mit getricksten Links
  - Browser-Hijacking
  - Keylogger/Sniffer

Phishing - Ausspähen von Daten



Ziel-Sektoren von Phising-Versuchen

Viren

Malware, Trojaner, Würmer, Bots

Viren

- Code, der anderen Code infiziert
- Wird beim Ausführen des infizierten Codes mit gestartet und verbreitet sich weiter
- Lebenszyklus:
  - Schlaf-Phase (verhält sich unauffällig)
  - Verbreitungs-Phase (versucht anderen Code zu infizieren)
  - Trigger-Phase (wartet auf Zeit/Datum oder anderes auslösendes Ereignis)
  - Ausführungs-Phase (führt die Schadfunktion aus)

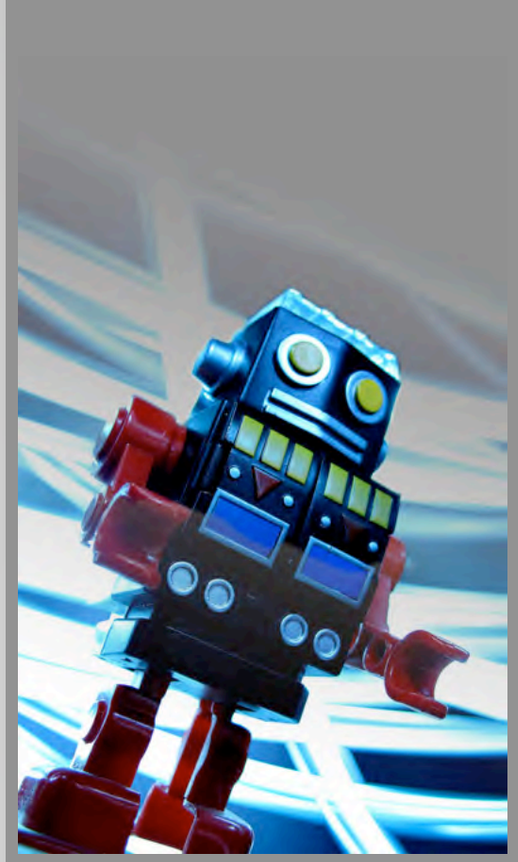
Trojaner

- Täuscht gute Absicht vor, Hauptzweck ist aber schädlich
- Verbreitet sich nicht selbst sondern wird von Nutzern aktiv installiert und verbreitet
- Installiert "Hintertür" im System
  - Fernsteuerung
  - Zugriff
  - Keylogging
- Beispiele für Trojaner-Verbreitung:
  - Screensaver
  - Tools für System-Tuning

Würmer

- Schadsoftware mit eingebauter Selbstverbreitungs-Funktionalität
- Ausbreitung im Netz meist rasant
- Meist eine Vielzahl von Verbreitungstechniken
  - E-Mail
  - NFS-Freigaben
  - CIFS (Windows) Shares
  - PHP-Skripte
  - Bugs in Datenbank-Server
  - Webserver-Bugs

Bots

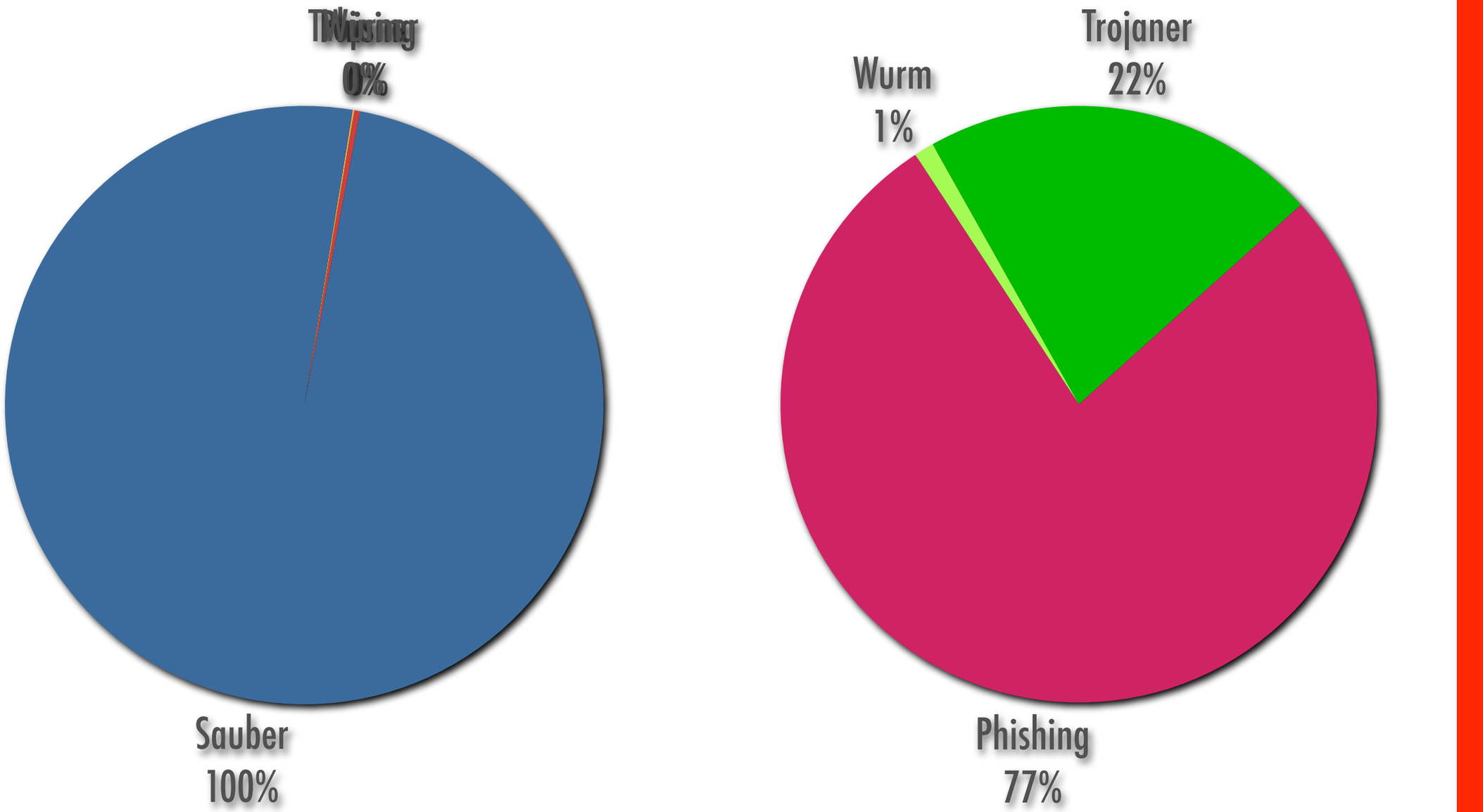


- Per Virus, Wurm oder Trojaner installierte Software mit Schadfunktion
- Wird über das Netz gesteuert
- Kann für vielfältige "Aufgaben" genutzt werden
- Wird auch "Drohne" oder "Zombie" genannt
- 85% aller Spam-Mails werden über Botnetze versendet

Problematik von Würmern, Trojanern und Bots

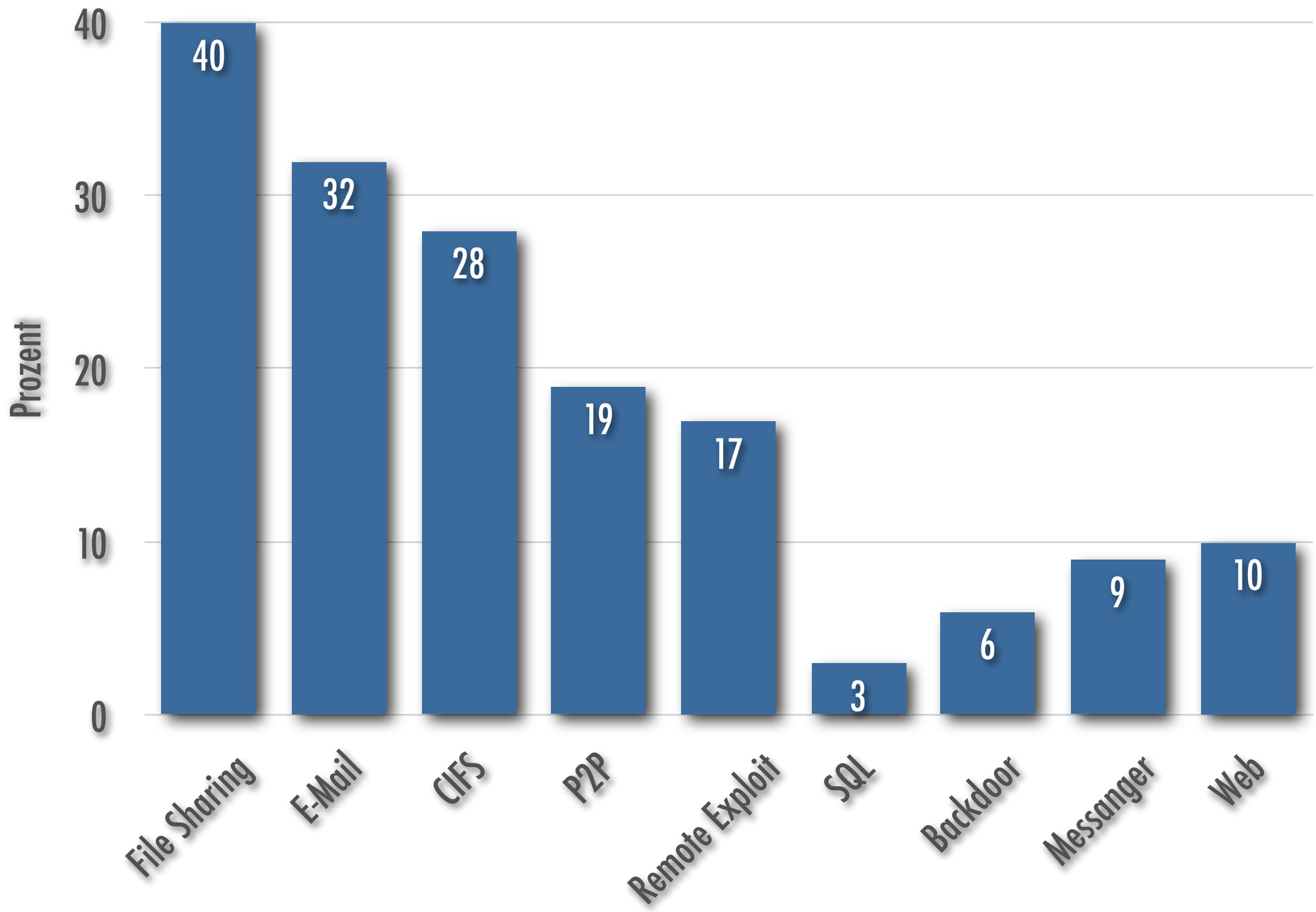
- Bieten Infrastruktur für eigene Verbreitung
  - Verbreitung beschleunigt sich selbst
  - Öffnen Türen für die nächste Betrugs-Masche
- Bringen Infizierte in Verruf
  - IP-Adressen landen auf Blacklisten
  - Absender ruinieren ihren Ruf
  - E-Mail-Adressen von Freunden & Geschäftspartnern werden verbreitet
- Schützenswerte Daten können ausgespäht werden
  - Passwörter
  - Kommunikation (E-Mail, Dokumente)
  - Kreditkarten- und Kontodaten

KNF Virus-Filter

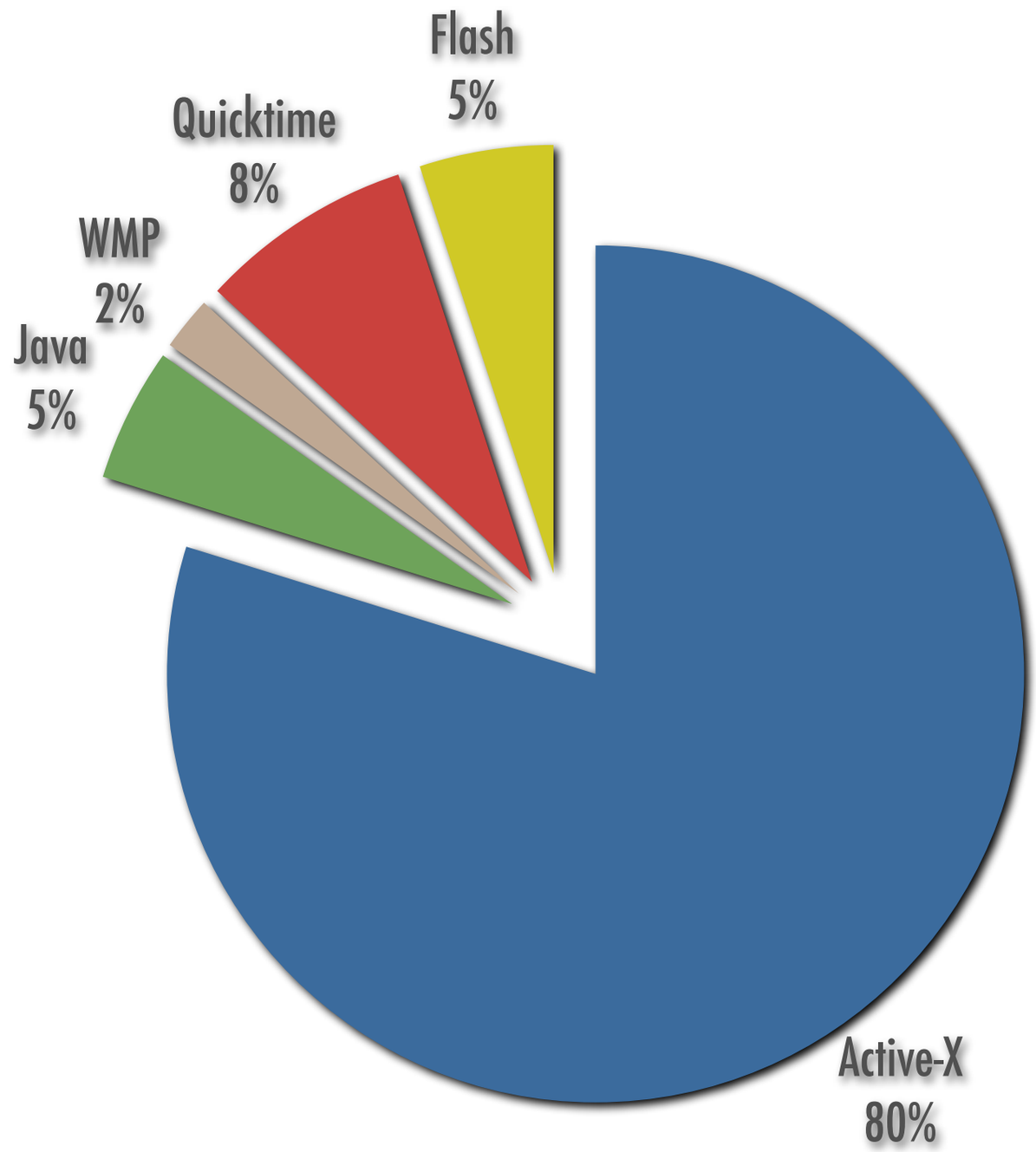


Virenscanner-Ergebnisse auf KNF Mailserver

Verbreitungsweg von Malware



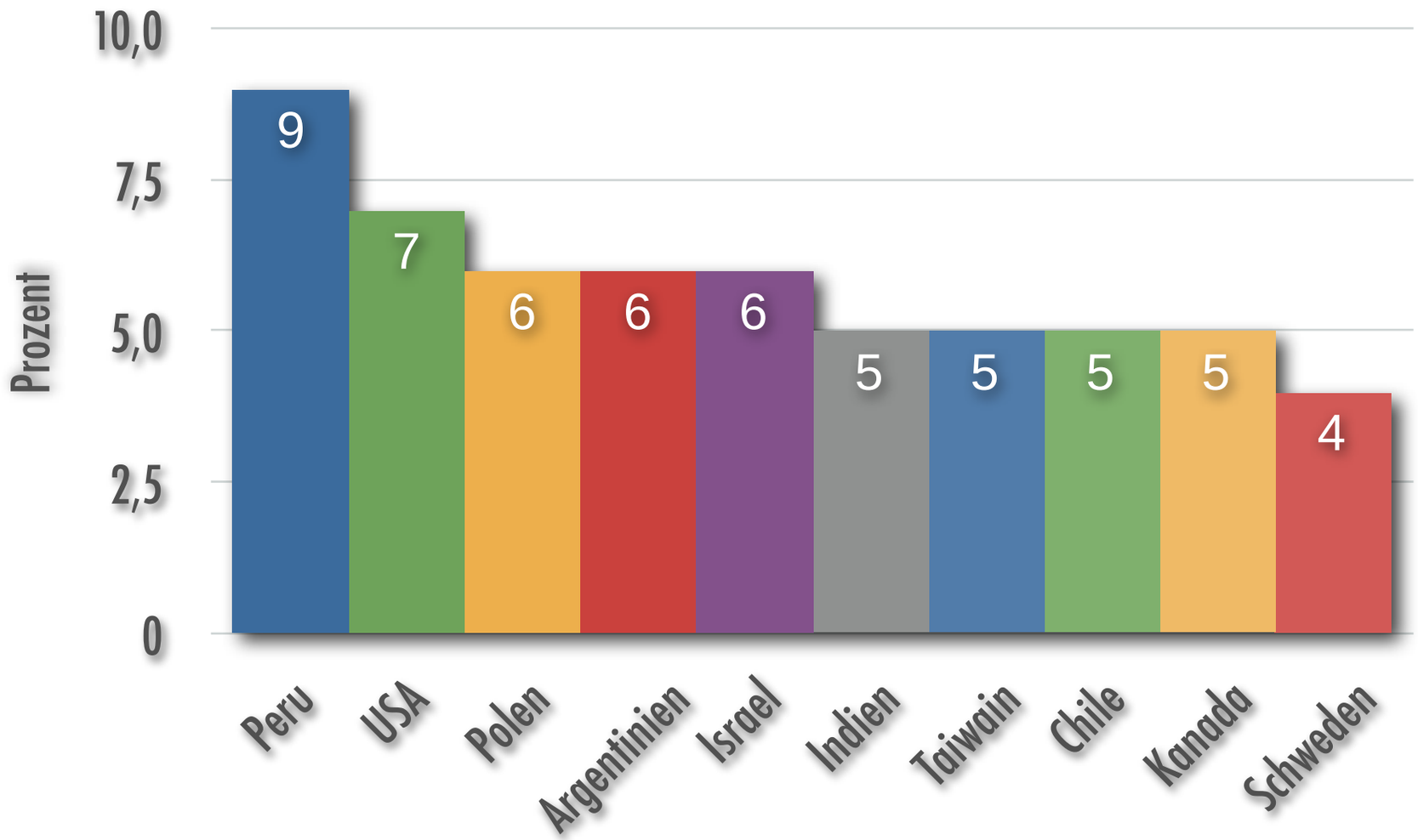
Verwundbarkeit durch Browser-Plugins



Viren und Würmer im Zeitalter des DSL-Booms

- Immer mehr Personen gehen online und können sich Software installieren
- Anzahl der über das Netz missbrauchbaren Dienste auf kaum gewarteten Rechnern steigt
- Missbrauchbare Bandbreite vervielfacht
- Bandbreite des Anschlusses von Privatrechnern übersteigt oft Firmenanschlüsse
- Von Würmern genutzte Bandbreite fällt kaum mehr auf
  - Viele Programme testen automatisch auf Updates oder "telefonieren nach Hause", Netzwerkaktivität ohne Nutzeraktivität ist heutzutage nicht mehr "seltsam"
  - In der verfügbaren Bandbreite führt die Mitbenutzung durch Würmer zu keiner merklichen Verlangsamung für den Nutzer

Bot-Quellen



Bot-Rechner in Relation zu Breitbandanschlüssen

Bot-Netzwerke

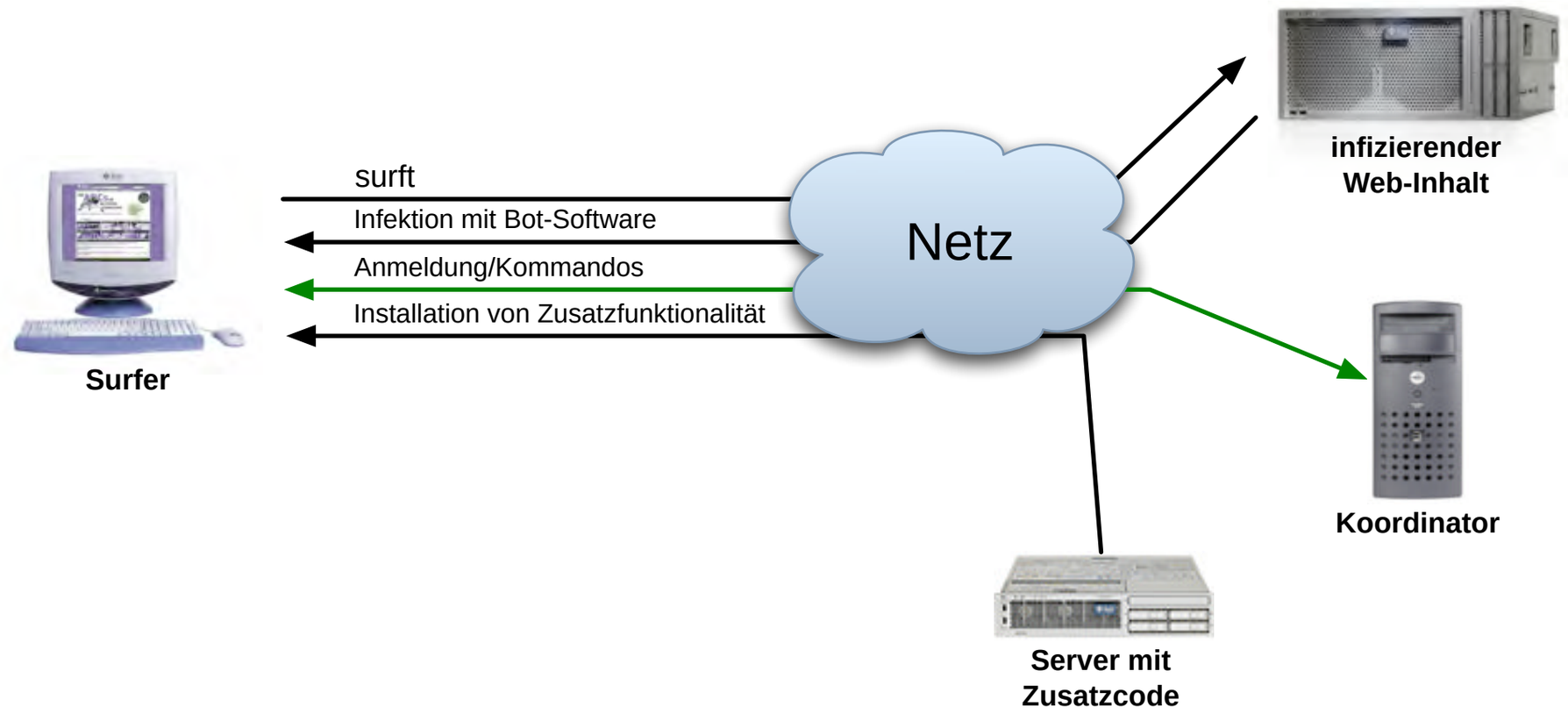
...gemeinsam sind sie stark

Bot-Netzwerke

- Bot-Netzwerke bestehen aus teilweise mehreren zehntausend Bots
- Microsoft's MSRT (Malicious Software Removal Tool) fand Trojaner auf 62% der 5,7 Millionen untersuchten Computer, die Mehrzahl hiervon waren Bots
- Nutzungsrechte können auf dem Schwarzmarkt gekauft werden
  - Exklusiver Zugriff pro Maschine 0,25$
  - "Shared" Zugriff pro Maschine 0,10$
- Universelle Werkzeuge für die Verbreitung von Spam, für Denial-of-Service-Angriffe, für das Ausspähen von Daten und das Verbreiten von Daten

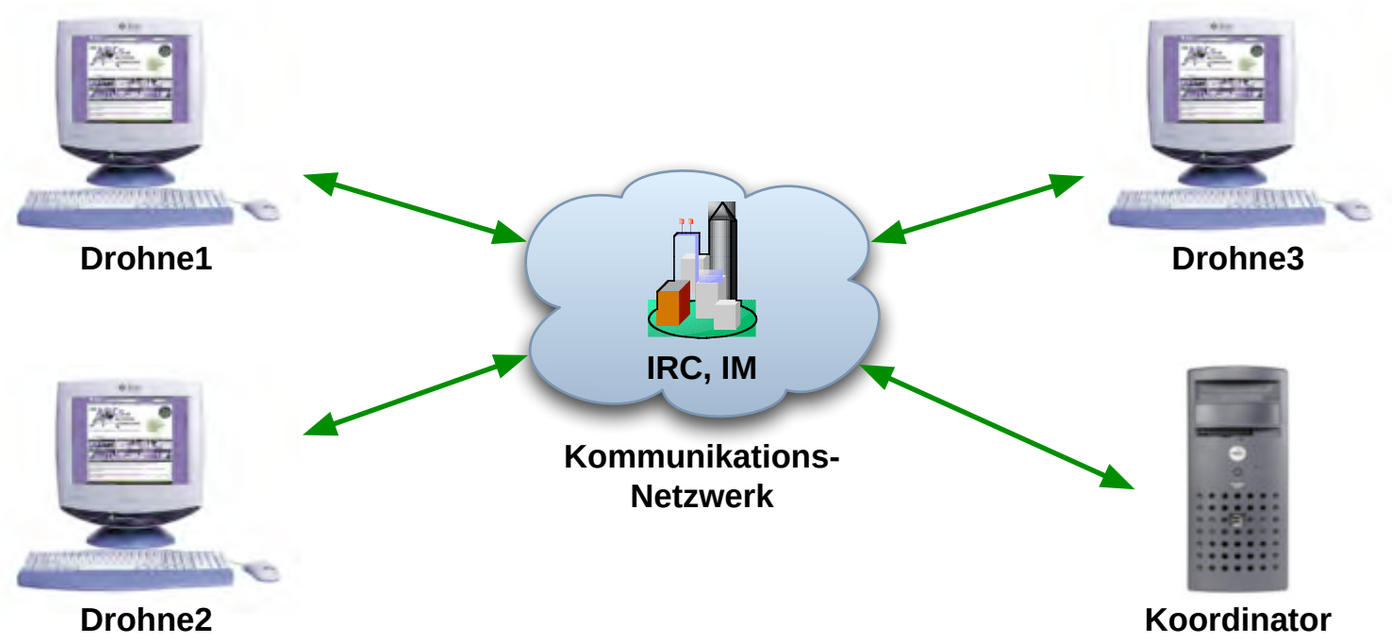
Bot-Netzwerke

- Die installierte Software enthält nur eingeschränkte Funktionalität
- Infizierte Rechner melden sich bereit beim Koordinator
- Koordinator gibt Kommandos, unter anderem zum Nachladen von Funktionalität

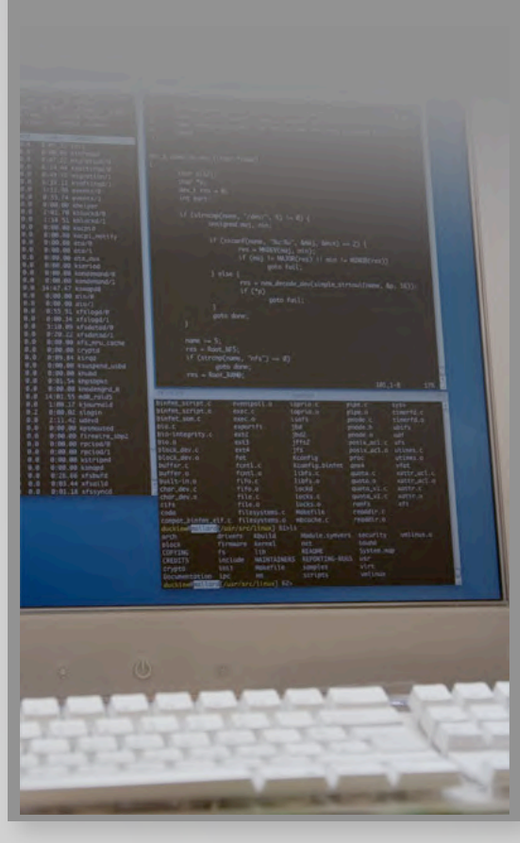


Bot-Netzwerke

- Koordinator will zum einen unerkannt bleiben und kennt zudem nicht die IP-Adressen neuer Drohnen
  - Registration über bereits existierende Kommunikationspfade
  - IRC, Jabber, P2P-Netzwerke - unauffällig da deren Nutzung nicht unüblich ist
- Ausfallsicher, da skalierenderes und in der Regel redundantes Kommunikationsnetz



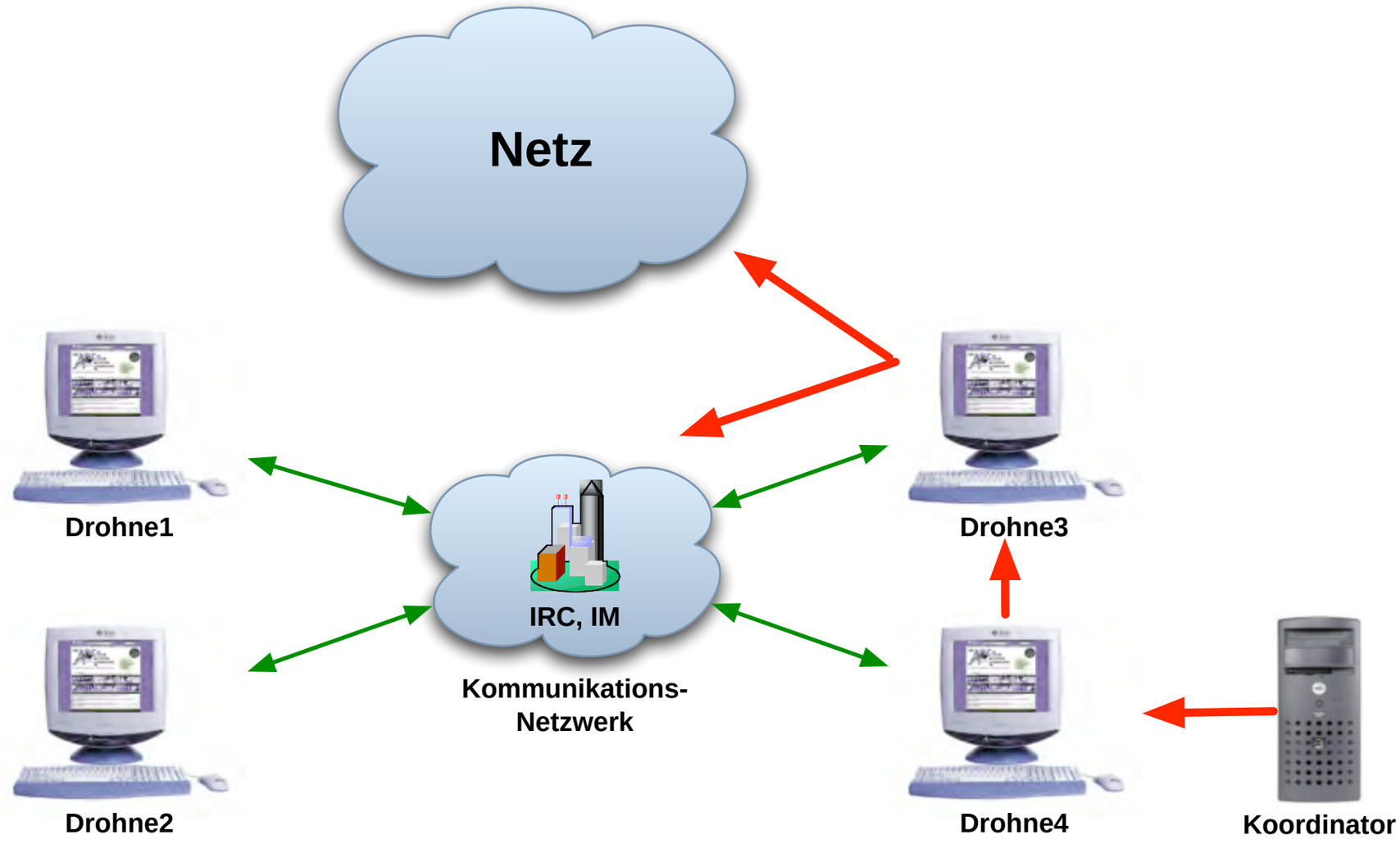
Bot-Software



- Datei-Download
- Starten/Stoppen von Programmen
- Infektion/Replikation
- Port-Weiterleitung
- UDP/Ping-Flood
- URL-Besuch
- Keylogging
- Spam-Erzeugung und Versand
- Netzwerk/Portscan
- HTTP-Server
- Socks-Proxy

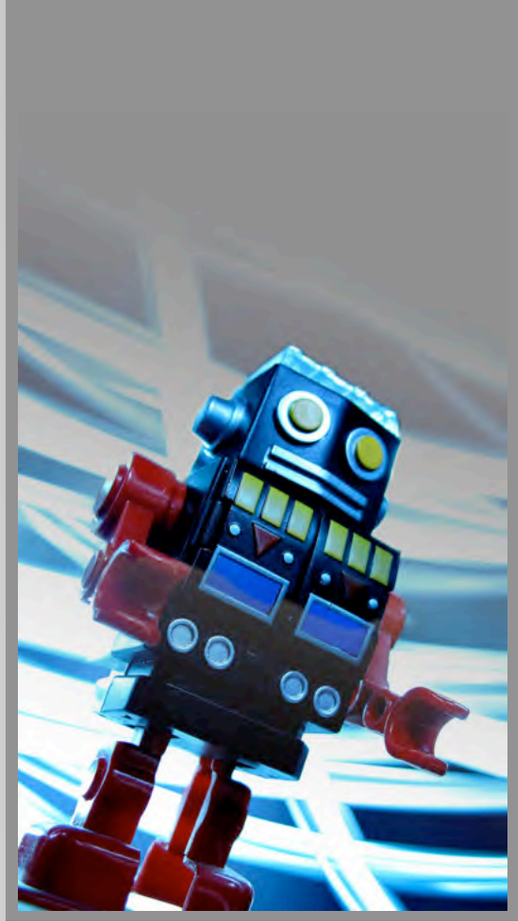
Bot-Netzwerke

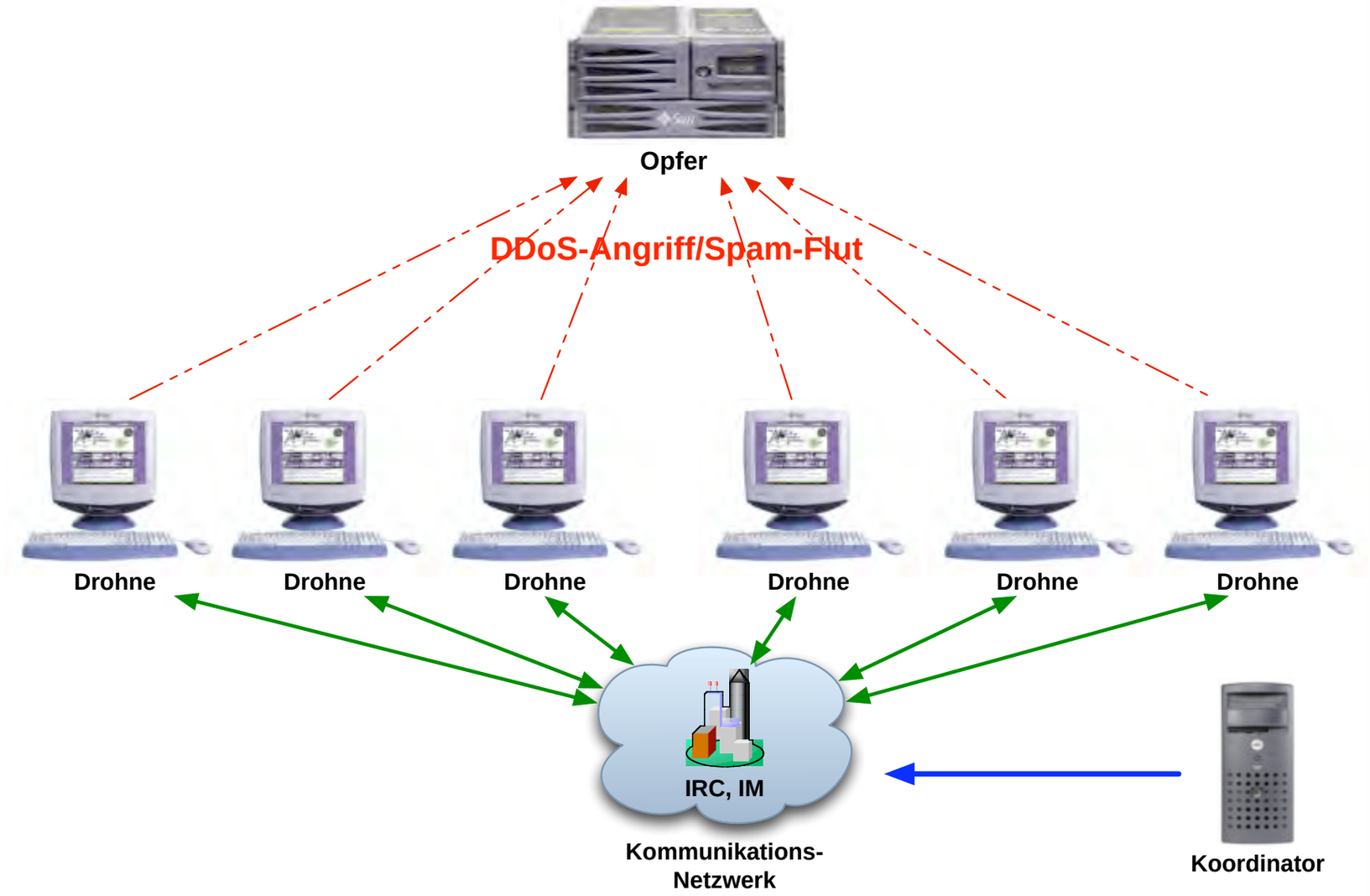
- Durch Proxy-Funktionalität können Identitäten verschleiert werden



Bot-Netzwerke

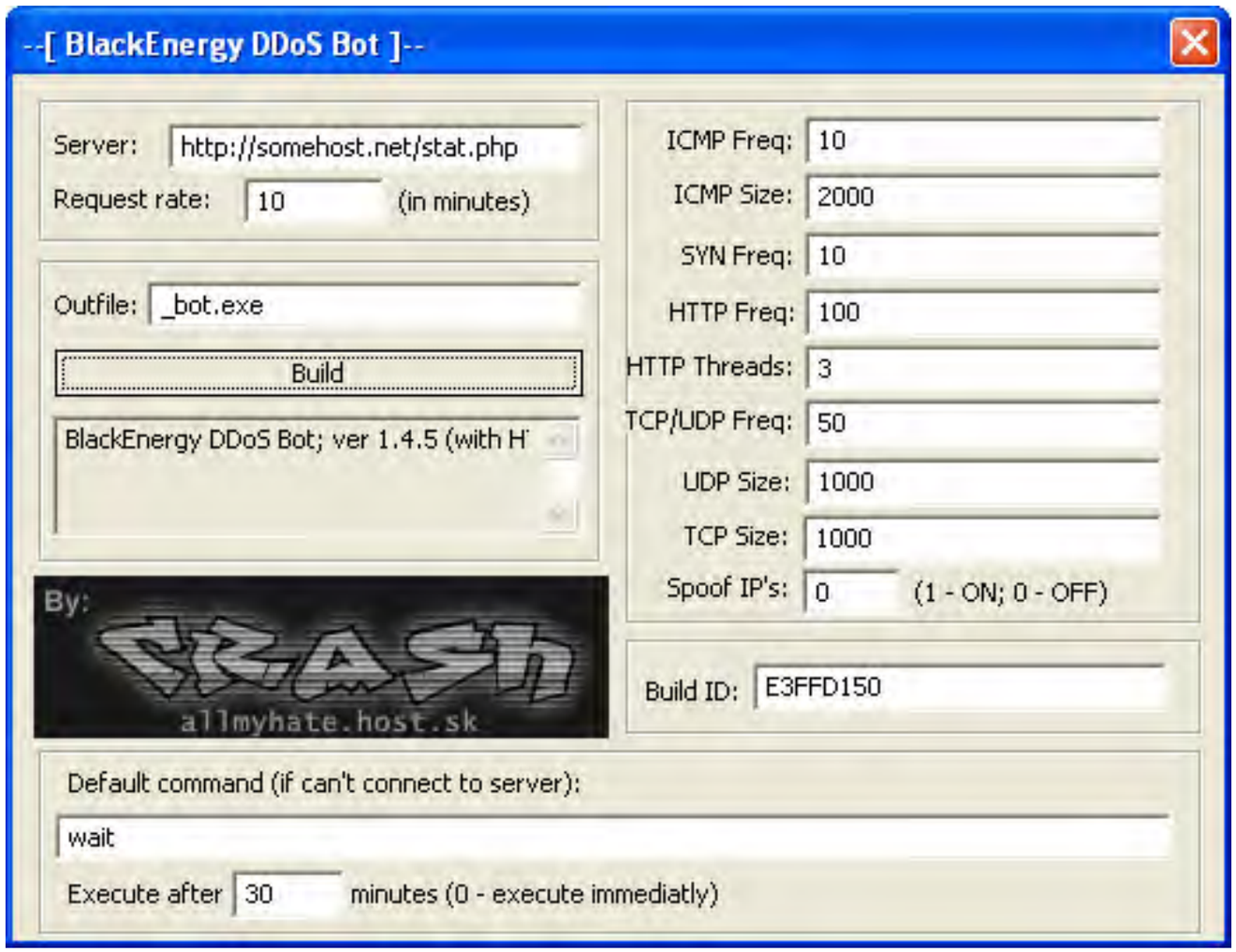
- Anzahl der Drohnen übersteigt die Kapazitäten selbst großer Dienstanbieter





Bot-Steuerung

- Einfache Bots werden mittels Konfigurations-File gesteuert



- Bessere Bots mittels HTTP- oder Windows-GUI

[statistics][control] [help]

[Global] [Downloaded files][Time statistics]

Zupacha Mini stats

	Protocol	Sent Msg	
B.	Spam-bots mail	1493082	80%
	Mirabilis ICQ	184027	10%
	E-Mail	181619	10%
	Web mail	10067	1%
	Aol AIM	809	0%
	Web forum	201	0%
	Yahoo! IM	189	0%
talk	Google Talk	3	0%

Tottaly Sent : **1,869,997**

Service name	Sent Msg	
mail.yahoo.com	5072	50%
mail.google.com/mail/	3240	32%
hotmail.msn.com	966	10%
webmail.aol.com	616	6%
Mail.ru	117	1%
rambler.ru	56	1%
comcast.net	0	0%
mail.com	0	0%
lycos.com	0	0%
earthlink.net	0	0%
care2.com	0	0%

Web mail Sent : **10067**

phpBB

Topic reply:

New topic messages:

VBulletin

Topic reply:

New topic messages:

Forum messages totaly: **201**

Top 20 Counries (see all)

Country	Rating	
Germany	10602	95%
Russia	179	2%
United States	81	1%
Austria	60	1%
France	26	0%
Switzerland	24	0%
Poland	19	0%
Spain	19	0%
United Kingdom	17	0%
Hungary	15	0%
Netherlands	10	0%
Czech Republic	9	0%
Belgium	7	0%
Mexico	6	0%
Brazil	5	0%
Iraq	5	0%
Italy	5	0%
Slovakia	5	0%
Turkey	5	0%
Greece	5	0%

Totally: **52**

Top 10 new counries today

Country	Rating	
Germany	25	93%
Czech Republic	1	4%
Russia	1	4%

totaly: **27**

Top 10 bot versions

Bot version	Rating	
3.2.7	11160	100%

Totally: **1**

Top 10 Countries order by bot`s reports

Country	Rating	
Germany	779693	93%
Russia	16807	2%
United States	11196	1%
Austria	5025	1%
France	3452	0%
Spain	3226	0%
Poland	1943	0%
Switzerland	1693	0%
Hungary	1474	0%
United Kingdom	1411	0%

Totally bot`s reports: **838750**

Sumarize

Bot`s count:**11160**

Today new bots:**350**

All New bot today:**27**

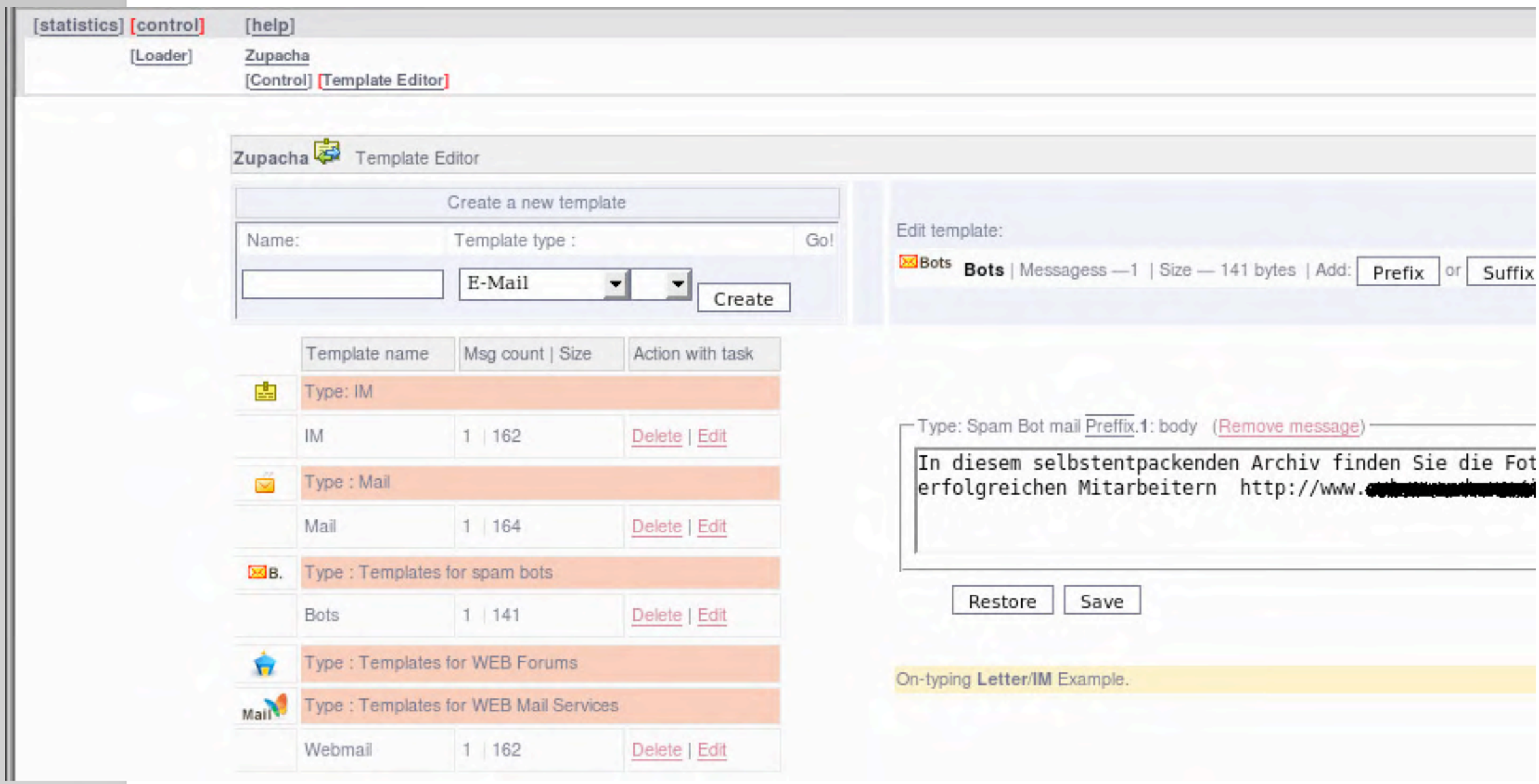
Percent Live bot`s: **50%**

Today Bot reports:**5596**

Bot reports:**838750**

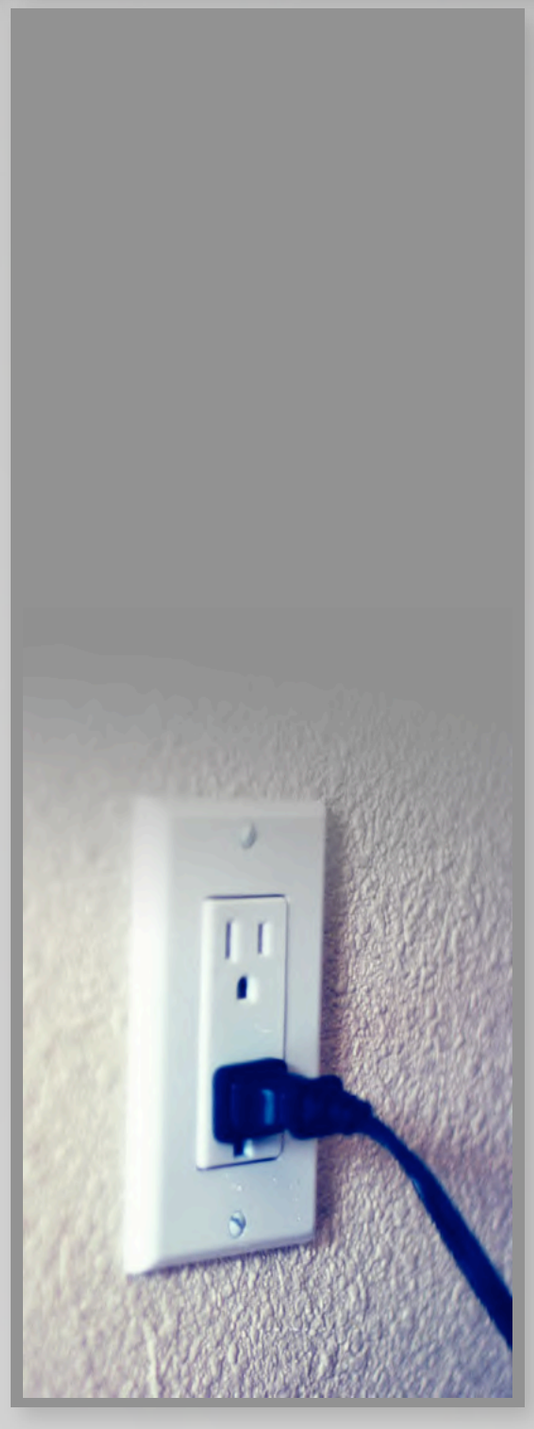
Oldest bot has: **19** days

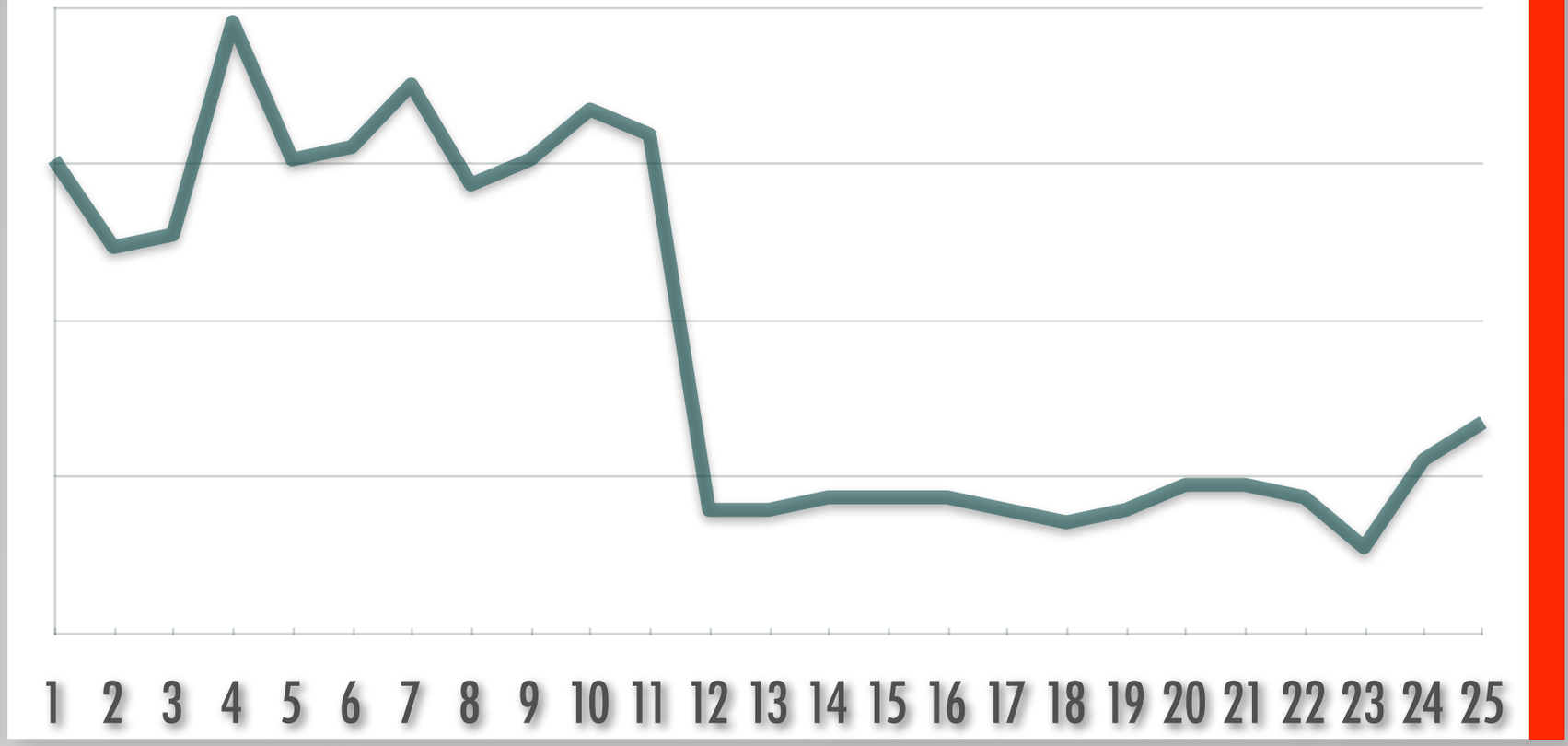
Zunker / Zupacha



Unplug McColo

- Colocation-Anbieter mit überproportional hoher Anzahl von Blackhats
- Wurde am 11. November "abgeklemmt"
- Botnetz-Drohnen laufen/liefen ohne Verbindung zur Kommandozentrale





Zukunft von Bot-Netzwerken

- Intelligente DDoS-Angriffe
- Intelligente Spam-Drohnen
- Echte P2P-Netzwerke
- Verschlüsselte Kommando-Kommunikation
- Schnelle Modifikation von Taktik und Technologie
- Fast Flux Hosting

Handelswaren auf dem "Schwarzmarkt"

Platz	Ware/Dienst	Anteil	Preis
1	Bankkonto	22%	$10 - $1000
2	Kreditkarte	13%	$0.40 - $20
3	Komplette Identität	9%	$1 - $15
4	eBay Account	7%	$1 - $8
5	Betrug	7%	$2,50-$50/Woche Hosting
6	Mailer	6%	$1 - $10
7	E-Mail Adressen	5%	$0,83/MB - $10/MB
8	E-Mail Passwörter	5%	$4 - $30
9	Drop	5%	10% - 50% des Betrags
10	Proxies	5%	$1.50 - $30

The End