



kpn



Rainbow-colored lists (white, black, green, grey,.....)

Run your very own DNS<IYFC>L

Someone Else's Blacklist

- Listing criteria
 - I do not like you
 - n hits on spamtrap
 - n virus received
 - n spam received
 - Via suspect mailserver
 - From suspect domain
 - You are already on blacklist X, now you are also on mine.
- Bailout criteria
 - Never
 - Pay up fee ('blackmail')
 - 'aging'
 - 'Friendly letters'
 - No questions asked, just react
 - bailout button on webpage

Why publish your policy (listing and ‘bailout’)

- If you don't : be prepared for lots of people ‘demanding’ a whitelisting
 - Especially bulk mailers (swearing they use double-opt-out)
- Published policy determines ‘quality’ for users of the list
 - Parties wishing to be listed
 - Parties wishing to use the list in their anti-spam solutions.
- Policy also needs to state criteria for de-listing
 - Providers turning to the dark side....
- A ‘governing body’ to handle exceptions and to execute delistings is advisable.
 - Especially when running a whitelist....
 - This ‘board’ could have members of welknown CERTs, the local ISPA.

The NLWHITELIST: an example

- Uses DNS for distribution
- Was initiated by o-IRT-o members after some incidents with providers blacklisting each other (spamfilters being too aggressive)
- Goal: diminish collateral damage caused by aggressive spamfiltering
- Listing Policy is published
 - Must be NL ISP or large organisation with lots of workstations
 - Banks, government agencies, universities
 - ‘must have own ASN and /20 worth of public IP space’
 - Outbound mailservers (smarthosts) are listed
 - Must have working abuse@ adres
 - [in consideration] Special provisions for bulkmailers and ‘hosted/housed mailservers’
- Contains about 1100 IPs.

Reporting formats in use or in study

- Lots of reporting is unformatted, using mail.
- ARF (Abuse-Report-Format) (AOL)
 - Mail-feedbackloops: standard complaint, offending mail attached
- Cymru format
 - 'pipe-separated' bulk report format (output of bulk-whois service).
- IODEF/IDMEF
 - Very elaborate XML spec, co-authored by Surfnet, RT modules exist
 - INCH working group in IETF is finalizing it.
- BIND zonefile format.
 - Format of choice in DNSBL world.
- ETIS project
 - Part of it is practical application of a reporting format.

Distribution methods

- Combination of a reporting format and distribution method
 - Distribution ('pull') via rsync/wget (list is published in some format on (web) server).
 - DNSBL method
 - Format is a DNS (Bind) zonefile
 - Information is distributed using 'pull' (from auth. DNS server)
 - Optionally: distribution ('pull') via rsync/wget (AXFR is expensive)
 - DNSBLs with >25M entries exist.
 - BGP method
 - Idea is to announce as a blackhole list for null-routing
 - Information is distributed using 'push'
 - Issues: someone else controls your routing policy (do you trust him enough?)
 - Can BGP really be 'misused' in such a way? Do we really want this?

Some standards

- Actually, there is none. There is no RFC on DNSBLs.
- 2.0.0.127.myblacklist.nl A 127.0.0.2
 - Indicates that the list is operational and maintained
- Use TXT records to indicate a reason.
 - 10.1.10.213.myblacklist.nl TXT 'this is a dirty spammer'
 - You can also return different 127.0.0.x codes, $x > 1$.
- Have a 'listing policy' and a 'bailout policy' ready
 - Use the txt records to publish the url of the policy pages.
- Use a short time-to-live (10-60 minutes) to keep the list dynamic
 - (but do not set TTL too short....)

Other possibilities of DNSBLs

- You can also do this with domain names, hostnames or URLs
 - Do not write them backward
 - Example: ***xs4all.nl.myblacklist.nl A 127.0.0.2***
- Ranges are possible:
 - ****.10.213.myblacklist.nl A 127.0.0.2***
- It does not need to be a BLACK list!
 - Whitelists, ‘dial-up ranges’, you name it.
 - A IP-to-Country system (return 127.0.x.y) with x.y the ISO country code, a number!)
 - A IP-to-ASnumber system (return 127.0.x.y) with x.y the AS number
 - See ***all.ascc.dnsbl.bit.nl***
- ENUM for telephone numbers also uses the ‘backward’ rule:
 - ***0201234567*** becomes ***7.6.5.4.3.2.1.2.0.3.1.e164.arpa***

Why is this DNS misuse?

- Most of the queries on a DNSBL are 'misses'
 - A 'miss' in DNS (host not found) is expensive.
 - One can do something with negative caching.
- Some Big ISPs 'subscribe' to a blacklist: master DNS server flooded.
 - Every mail will trigger a DNS lookup
 - These all tend to go the master of the DNSBL domain
 - Looks like a dDoS attack.....
- Big ISP subscribes to many blacklists: melts its own DNS server....
 - Same happens if their customers use DNSBL based spamfilters....
- Solve this by running multiple slaves, mirroring, and the like.
- DNSBLs typically have low TTL (10-60 minutes)
 - frowned upon by DNS admins
 - (lost of zone transfers, defeats caching mechanisms)

The 'Trusted Complainer' model

- Abusedesks send each other complaints in BULK.
 - I (sending party) will send you the incidents your customers caused in my network/platform.
- Improve resolution of the 'abuse-detection radar' of the receiving party
- Receiver determines the quality and reliability of the complaints
 - Is part of the abuse policy of the receiving party.
 - For instance: external complaints must correlate to internal complaints.
 - Receiving party may assign different quality factors to senders.
 - Sending party cannot 'demand' anything, but it can acquire a reputation factor
- Sending parties can be others than abusedesks
 - Anti-virus companies, generic blacklist managers (spamcop etc), regulators
- Privacy issues????
 - (like in exchange of blacklists of non-paying customers by telcos)
- The reports must be exchanged in a machine readable way (for automation).

Operating a blacklist and the trusted complainer

- If you publish your blacklist to the world
 - You will be held responsible for blocking mail
 - Even on mailservers you have never heard of yourself.
 - Your list may be used in a way you did not intend it to be used
 - You get a lot of 'hate' mail from people demanding delisting or people who do not want to understand how your bailout policy works
 - Your DNS server (being the authoritative server) cannot handle the extra load
- Possible Solution:
 - Use the trusted complainer model.
 - If someone else wants to use your list, he will get only the IPs in his domain.
 - If you block outside your domain, you should have the 'evidence' yourself. (or at least be able to get to it in an easy way)
 - Complaints probably will go easier to the mailserver manager.
 - This stimulates to do 'own' measurements

Questions

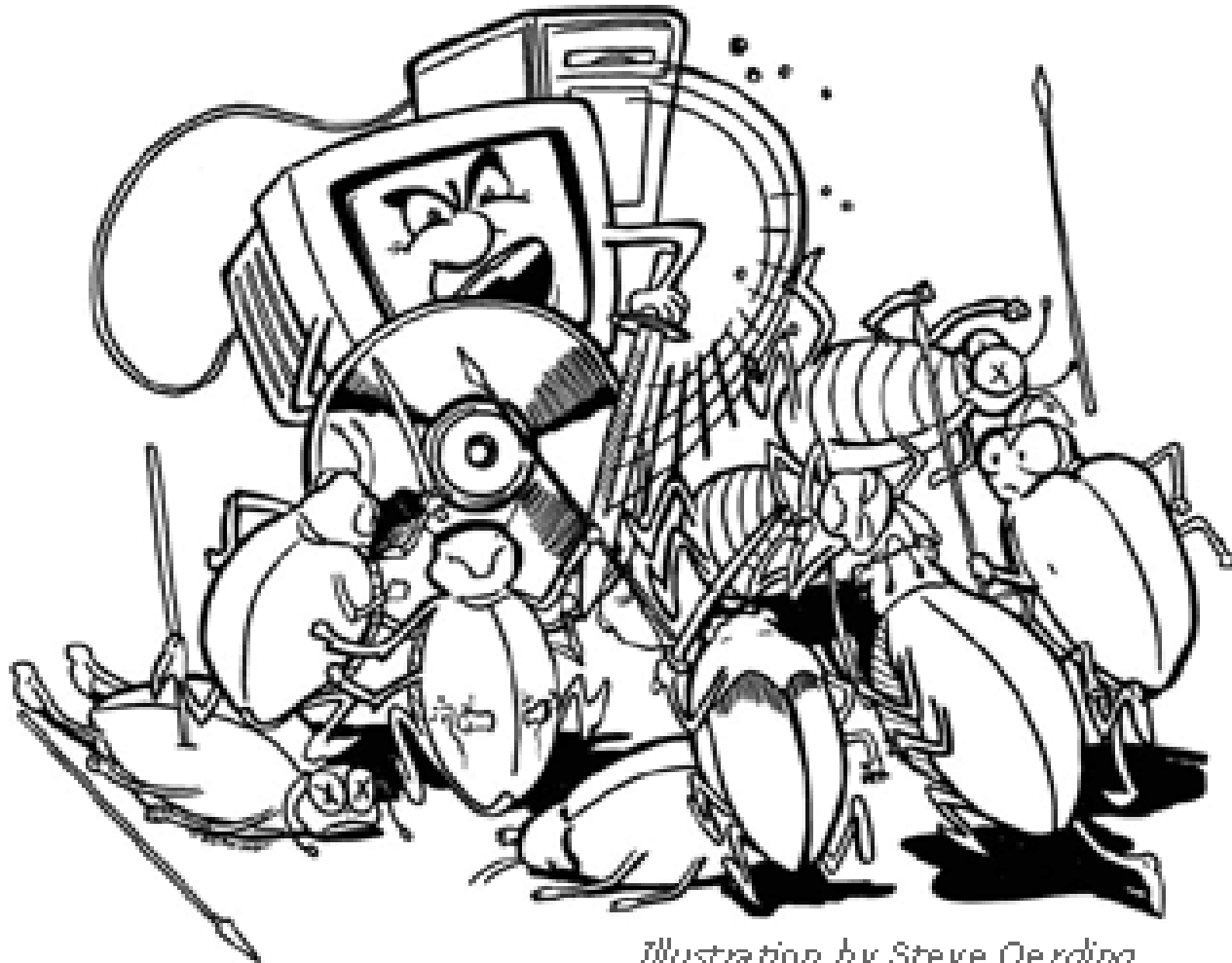


Illustration by Steve Oerding