IP ADDRESS BLACKLIST REMOVAL SOLUTION FOR INTERNET SERVICE PROVIDERS

Author: DSCC

Data Consultants Corporation
600 N. Commons Drive
Suite 100
Aurora, IL 60504
Tel: 630-692-2702
Fax: 630-692-2730
Email: spal@dccil.com
It may be possible that the PC/network has been infected with a virus and used to send spam without the owner’s knowledge. The spam appears to come from owner’s IP address and is therefore blacklisted. These Open-relay blacklists are based on open ports through which unauthorized network traffic is allowed to flow. Open-relay blacklists are the most widely used. Many of the better blacklists will run an automated script to verify that the evidence against owner is genuine before blacklisting owner’s IP.

A blacklist organisation will also list much larger blocks of IP addresses than those owned by the suspected abuser. So, if the owner is provided with an IP address and the spammer owns an address that is close in range to the owner’s and the spammer gets listed on this type of blacklist, owner’s IP address might be listed as well. Usually the reasoning behind this practice is that, by punishing innocent parties, the blacklister is putting more pressure on the ISP to disconnect the suspected spammer’s Internet access.
Why would a Service provider bother?

IP address blocks used by the subscribers are owned by the ISPs. The IP address blocks are assigned to the ISPs by registering authorities like APNIC/ARIN. If these IP address blocks generate SPAMs very frequently, the whole AS number assigned to the ISPs are blacklisted by the blacklisting services available worldwide. After AS blacklisting, even addition of new address blocks to the existing AS gets blacklisted very soon because of bad reputation of the AS. Tolerance score assigned to such AS is set very low by the blacklisting services.

As a result of blacklisting, the users’ SMTP requests are blocked by the email servers worldwide. This leads to DoS with respect to outbound email service. ISPs keep on receiving number of complaints from the users regarding this every day. Even if the ISPs de-list the specific IP addresses leased to the subscribers from the different blacklisting services like Spamhaus etc., it does very little to solve the problem. It becomes a multistage problem for ISPs to carry out such practice as a regular process because of the following.

- De-listing is allowed by the blacklists against one single IP address per request. For de-listing of one single IP address, number of blacklisting sites needs to be visited to submit the form of de-on every individual site. Also, de-listing process involves exchange of emails to verify authenticity of de-listing request. The de-listing process varies from one blacklisting site to another. De-listing one IP address from all the blacklists may require several hours of background processing.

- De-listing is not allowed in ‘per subnet’ basis.

- If the De-listed IP Address belongs to a blacklisted AS, the reputation score for this de-listed IP address would be set as ‘BAD’ by the listing servers. This would lead to very low SPAM tolerance by the listing servers for the de-listed IP address. It is seen that even if a very few SPAM emails are generated from such a de-listed IP address again, it gets re-listed in no time.

- Every time an IP address gets re-listed after de-listing, its reputation score is further lowered. After a certain number of re-listing after de-listing, the de-listed IP address enters into ‘permanent listing’. This problem might be nightmarish for an ISP and a subscriber because in such case, the ISP has to provide the concerned subscriber with a new set of different IP addresses.

- If the IP addresses are assigned to the subscribers through DHCP, the problem becomes more complex in nature because one ‘recently cleaned’ IP address may be allotted to an infected PC generating huge SPAM.
What are the trivial solutions available?

- **Free De-listing Service:** The ISPs cannot afford to provide clean IP addresses by the process of de-listing. It is impractical for thousands of IP addresses. Even if ISPs want to move ahead with de-listing the listed IP addresses whatever the pain may be, each de-listing require multiple hours of background processing.

- **Using Mail servers:** If ISPs mandate the users to use a specific mail server for outbound emails from the subscribers this would add complexity in the operation of subscriber roll out. This may lead to huge administrative overhead because every user’s desktop email client needs to be configured. There are lot of ISPs for whom this may be a mammoth task. Also if the subscribers’ PCs are infected with the Trojan horse malwares those use the existing email clients on the subscribers’ desktops to generate SPAM, lots of SPAM will exit from the ISP network bearing the source IP address as that of the email server. This will lead to blacklisting of the e-mail server itself leading to DoS of outbound email services for the entire ISP.

- **Drop SMTP:** Dropping outbound SMTP on the gateway router might seem to work initially for some time but it makes the network inflexible because the users are not allowed to use their own SMTP servers in this case. The ISPs who provide ILLs to companies would not be able to go for this practice because of SLA.

- **Paid De-listing:** Rapid de-listing of IP addresses is possible through some online services. These services cost considerably for every de-listing attempt.
How do we solve this?

**Spam Identification:**
- Monitors all outbound SMTP traffic from subscribers of the ISP.
- Scans for SPAM e-mails and block them allowing only good emails to go.
- Blocked e-mails would remain stored in the system for 14 days.
- ISP may inspect the SPAM emails, detect false positives and release them.
- Mail search interface for the ISP.

**Almost Nil Administrative Overhead:**
- No special configuration on the subscribers’ computers. It works in stealth mode and is not visible to the users.

**Local Blacklist inside the ISP:**
- IP addresses of subscribers sending large amount of SPAM is blacklisted.
- Creates private, automated blacklist for the ISP.
- Interface to monitor IP addresses blacklisted.
- Interface to temporarily release the blocked IP addresses.

**Infected node identification and Logging:**
- Identifies nodes infected with spamming malware and blacklists them.
- All SMTP traffic is dropped from such nodes.
- All SMTP transactions are logged.

**ILL friendly solution:**
- Does not require generic blocking of SMTP.
- Can be deployed for ILL gateways.
What is the Solution Architecture?

The solution supports the following deployment modes:

- Central
- Distributed
- Clustered
- HA

The clustering feature allows the solution to Scale up to whatever size it requires to be. The most popular deployment mode is shown below.

What are the Solution Components?

- **Hardware:** ISP provides suitable server hardware.
- **Software:** White-wash
- **Alerting service:** MXToolbox