

## **Response to the OFTA Consultation Paper, “Proposal to Contain the Problem of Unsolicited Electronic Messages”**

by Hong Kong Computer Emergency Response Team Coordination Centre

### **1. General**

We consider that a combined approach with legislation, technical measures and user education will be most appropriate approach to tackle the unsolicited electronic messages or unsolicited bulk e-mail (UBE) issue.

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) which was mentioned in the consultation paper (paragraph 50), considers that the centre can contribute to user education, but may not be a suitable party to operate and maintain the local Real-time Blackhole List (RBL). HKCERT can also assist in cross border communication with CERT teams around the world on resolving spamming issues.

### **2. User Education**

HKCERT has organized public seminars in information security topics including issues on spamming. The centre possesses good understanding of the spamming issue and constantly received reports on spamming. The centre has also established good communication with local Internet Service Providers (ISPs) and a good subscriber base to propagate and disseminate information. It will be a good channel to promote the awareness and provide user education to the general public.

### **3. Cross border Communication**

The global CERT team community has become more mature. The CERT teams act as a bridge for resolving cross-border security incidents. They can also leverage on such communication infrastructure to ease the report and resolution of cross-border spamming cases.

When a party wants to locate a spamming source across the border, they can seek help from the local CERT team, which will in turn contact the CERT team

responsible for the region of the spamming source for assistance. CERT teams can usually help identify the ISP responsible and negotiate with the ISP to take the appropriate actions.

#### **4. Real-time Blackhole List (RBL)**

##### **4.1 Background**

- RBL is a list of email servers IP addresses which are believed to have connection with UBE. RBL can be categorized into SPAM RBL and or Exploit RBL. Spam RBL contains those direct UBE sources and verified spam services. Exploit RBL are illegal third party exploits, including proxies, relays, worms and Trojan exploits.
- The RBL services employ a framework based on the domain name service (DNS). The blacklisted server IP addresses are implemented as a DNS zone file. When a subscriber wants to check the status of a mail server, she makes a query to the RBL server with the mail server's IP address. The RBL server responds to the query an IP address with a code which indicates the status of the IP address as "not in the list", "is a Spam RBL member" or "is an Exploit RBL member".
- Mail server configured to use RBL will block the communication with the IP addresses on the list, unless the system administrator overrides with an alternative policy. In this way, the subscriber can save network bandwidth communicating with the UBE sources. They also save CPU time to process and server disk space to store the UBE.
- Most RBL users are ISPs, network operation centres, big corporations and universities.

##### **4.2 Functions of RBL Service Provider**

- RBL Service Provider provides the technical infrastructure for subscriber to make query and copy the blacklist. She has to ensure the infrastructure is available all the time, like the DNS services. She also needs to ensure the blacklist is updated and accurate all the time.
- RBL Service Provider also needs to provide a sound and transparent investigation procedure to validate the complaint reports and to monitor the response actions of the complained IP addresses.
- RBL Service Providers also provides a sound administrative and communication infrastructure to handle report of Spam or Exploit IP

addresses, to handle counter-report and appeal from the owners of complained IP addresses.

#### 4.3 Operation Processes

- **Report** –The RBL Service Provider has three major ways to receive reports of “bad” IP addresses. Firstly they can put email probes around major Internet networks to collect and analyse spam sources. Secondly, they can subscribe such information from other sources that are mostly anti-spam filtering service providers. The last way is from received complaint reports filed by complaining parties. When a user wants to report a bogus IP address to the RBL Service Provider, they have to follow a defined procedure to submit the complaint with proof.
- **Verify** – The RBL Service Provider verifies the complaint with investigation tools. They classify the reported IP address according to the specified criteria. If a case is established, she will add the IP address in the RBL. The RBL Service Provider provides an efficient interface for the public to enquire if an IP address is on the RBL.
- **Handle Request for Removal** – Some RBL Service Provider will try to contact the owner of the blacklisted mail server but many do not do so to save resources. When the owner blacklisted server discovered they are on the RBL, they can get their names removed by either appeal to RBL Service Provider with good reasons, or by proving that they have rectified the situation and their email server will no longer send out UBE.
- **Maintain** - When the RBL Service Provider is satisfied with the complained IP address is no longer sending out UBE, they can manually remove it from the blacklist. If no action was reported by the RBL listed item, they are still ways to maintain the list to good shape as time goes on. Some RBL Service Provider uses an automated script to re-scan the blacklisted IP addresses periodically to removed corrected mail servers from the list. Some uses expiry time, say 6 months, to remove items from the list without investigation.

#### 4.4 Resources Requirements

- RBL services are operated by either commercial entities or non-commercial entities. Commercial entities charge a fee to subscribers. They are able to sustain and provide continuous improvement to their service. Spam blacklist service is not a cheap service. Non-

commercial entities got funding support from other organizations or by donation.

- RBL operations require a lot of resources, including the human resources to handle ongoing communications with reporters of UBE and respondents, to administer the blacklist and to provide technical support to the technological infrastructure. The staff of which should be experienced in handling complaints and appeals with good communication skills.

#### 4.5 Liabilities

The RBL Service Providers live with complaints and appeals all the time because there is no bulletproof way to guarantee a 100% correctness in the classification of UBE source. Some RBL Service Providers provide a consolidated list from several RBL sources from different regions of the world. It is even harder to guarantee quality of the RBL. RBL Services Providers usually disclaim the liabilities in using the blacklist. However, the service provider must prepare for settlement of disputes raised.

#### 4.6 RBL development in Asia Pacific

- In mainland China, the Internet Society of China (ISC) which is the forum of internet network providers in China, had recently formed the Anti-Spam Coordination Team which publishes the mainland China's RBL. References can be made to:
  - <http://www.isc.org.cn/20020417/ca226065.htm> (English)
  - <http://www.isc.org.cn/20020417/ca172562.htm> (Simplified Chinese)
- In Taiwan, there is no local RBL. In February 2004, some big ISPs of Taiwan set up an anti-spam team to react to spamming. One of their plans is to set up Taiwan's RBL and coordinate with international organizations to deal with spams. In the university academic network, the Taiwan Academic Network (TANet) is currently taking the responsibility of the academic network RBL.
- From this trend, the network provider community is taking up the task of RBL. The advantage is that the RBL managing authority has close relationship with individual network providers. The efficiency of the response mechanism is very high. The down side to this approach is that the RBL is not managed by a third party, the RBL operating organization needs to deal with internal conflicts.

#### 4.7 CERT teams and RBL Service Providers

- We are not aware of any CERT team directly operating a local RBL.
- We consider that a CERT team is not a suitable party to operate the local RBL because:
  - (a) Nature and Expertise of CERT is different from a RBL service organization
    - CERT is a small and compact team, focusing on virus and security incidents that need immediate attention. The nature of these problems requires in-depth analysis and technical advice to fix the problem as quickly as possible. Staff of CERT teams tends to be technical.
    - RBL authority deals with continuous communication and handling of complaint and appeals. The staff does not require in-depth technical skills, but good communication skills are necessary.
    - The nature of business is different and the skills required are also different. There is no saving for the functions to be grouped under one roof.
  - (b) The operations of RBL service will require a separate infrastructure to support that cannot usually combine with existing infrastructure running a CERT team.
  - (c) The primary function of a CERT team is to handle security incidents. With the increasing complexity of virus and security attacks, CERT teams should put more effort to better develop herself as the coordination centre of local security incidents, and enhance its relationship with local stakeholders and the international CERT community. RBL administration will distract the focus of the CERT team.
  - (d) A different source of funding must be sought to operate the RBL service, either from subscribers or other sources

#### 4.8 Conclusion

- HKCERT is not an appropriate party to operate the local RBL
- We would suggest that the local RBL service provider, if any, should be

operated by a neutral and reputable body with sufficient resources to operate and a close collaboration with the ISPs and network providers.

-- END --