Microsoft Spam Enforcement
Fact Sheet and Observations
Revised May 18, 2007

- Microsoft has filed **128** lawsuits in the US against spammers.
  - **357** defendants have been named, including:
    - **236** individuals
    - **121** corporate entities

- Microsoft has filed **89** lawsuits in the US against spammers under CAN-SPAM.

- Microsoft has filed **82** lawsuits against John Doe defendants.

- Microsoft has amended **39** cases to name defendants in John Doe spam lawsuits.

- Of the **128** lawsuits filed in the US against spammers, MS has reached the following resolutions:

  - **35** cases with defaults or stipulated judgments
  - **12** cases with defendants filing for bankruptcy
  - **48** cases with settlements
  - **3** summary judgments
  - **42** cases dismissed with no judgments or settlements

- Of the **128** lawsuits filed in the US against spammers, **17** of the defendants were listed on the Register of Known Spam Operations (ROKSO) and **6** of these **17** defendants were included on ROKSO's top 10 list.

- In total, Microsoft's anti-spam enforcement activity has produced **more than 200** worldwide legal actions. In a number of these actions, Microsoft worked with governments outside the U.S., in countries throughout Europe, Asia and South America, to either file lawsuits or identify and drive enforcement activity against spammers.

- Microsoft has partnered with government, law enforcement and industry partners to file lawsuits against spammers, including:

  - State Attorneys General Christine Gregoire (Washington/June, 2003) Eliot Spitzer (New York/December, 2003), Gregg Abbott (Texas/January, 2005), Charlie Crist (Florida/April, 2005), Bill Lockyer (California/April, 2005), Tom Reilly (Massachusetts/May, 2005)
  - Strategic Policy Manager Ian Bourne of the United Kingdom's Information Commission (June, 2003);
  - Industry partners AOL, EarthLink and Yahoo! (March, 2004 and October, 2004)
  - Amazon.com (September, 2004)
  - Pfizer (February, 2005)
  - Federal Trade Commission (May, 2005)

Observations

The Evolution of Spam Enforcement

In the many years during which Microsoft has been involved in civil and criminal enforcement, the techniques used by spammers have evolved. As a result, some of the enforcement techniques that were most effective are no longer viable; finding and prosecuting spammers is more challenging in today's environment.

Some of the observed changes are:

- Affiliate program operators, who provide the economic engine for spam, rotate their URLs much more frequently, sometimes on a daily basis. Similarly, spammers no longer advertise the URLs provided by the affiliate programs. Instead, they include throw-away domains as links in their spam and use those domains to redirect to the URLs provided by the affiliate program.

- The use of image spam makes it much more difficult to locate and retrieve related spam. For the same reason that image spam impairs an ISP's ability to filter, it also foils the enforcement tools that allow the identification and collection of spam from customers or trap accounts – namely, image spam lacks a searchable URL, reliable HTML pattern, or other machine readable data that permits easy identification and retrieval.

- There has been a growth in spam that does not contain a link to, or vehicle for, selling a product but, instead, simply advertises a product. A good example is stock spam. The spam message touts the product, but does not provide a method for acquiring the product. Because the sale occurs in a channel unrelated to the spam, an investigator can not "follow the money" from the spam message.

- Most illegal mail is sent through open proxies, and especially through compromised computers that are part of botnets. Very rarely are illegal messages sent through dedicated pipe. Likewise, very few advertised domains are registered or hosted using U.S. companies; the ones that are have often been purchased by persons outside of the U.S. and/or through stolen credit cards.

- While many spammers still live in the U.S., they have easy access to overseas banking facilities, IP addresses, bullet proof hosting and payment processors.

In general, the implementation of CAN-SPAM and related state statutes has polarized the emailing community. Many emailers have abandoned their prior deceptive practices but are emailing with renewed vigor, flooding the inbox with CAN-SPAM-compliant mail. Other spammers have continued to send deceptive mail, and have now grown more sophisticated in their operations. The enactment of these statutes, and particularly the availability of criminal penalties, has seemingly discouraged the formerly large collection of "amateur" mailers.

Current Challenges in Spam Enforcement

- "Downstream" targeting (i.e. attempting to "follow the money" generated through sales of the advertised product) – is still a viable technique. But the use of image spam, rotation of URLs, and use of offshore resources have diminished its success. Cyber forensics is becoming less effective in locating the programs for which spammers advertise; however, standard investigative techniques and the use of informants are still viable for penetrating the complex operation of affiliate programs.

- Because the vast majority of illegal spam is sent through open proxies, "upstream" cyber investigation (i.e. attempting to identify the sender through investigation of the computer that delivered the spam) is not viable absent use of a compromised computer. That is, the true sending location of spam can only be determined by controlling and analyzing one of the computers that has been compromised and is being used as part of a spamming botnet. This in turn requires the establishment of a honeypot, a robust set of infection vectors, and a powerful analytical tool.