Dear Network professionals:

We are writing on behalf of an international group of government agencies to request that your organization join a worldwide effort to prevent spammers from compromising consumers' computers and using them as "spam zombies." Our agencies are responsible for combating illegal spam through law enforcement, technical research, consumer and business education, policy development, and public-private partnerships.

Spammers use home computers to send bulk emails by the millions. They take advantage of security weaknesses to install hidden software that turns consumer computers into mail or proxy servers. They route bulk email through these spam zombies, obscuring its true origin.

As an Internet Service Provider (ISP), your organization has an interest in the integrity of the email system, which is threatened by the onslaught of spam routed through spam zombies. In addition, recipients may blame your organization for spam that appears to have originated from your system, or your customers' systems. And the spam may cause your network connections to bear unnecessary loads, increasing your administrative costs.

We encourage you to implement these voluntary anti-zombie measures if you are not already doing so: [1]

- block port 25 except for the outbound SMTP requirements of authenticated users of mail servers designed for client traffic. Explore implementing Authenticated SMTP on port 587 for clients who must operate outgoing mail servers.

- apply rate-limiting controls for email relays.

- identify computers that are sending atypical amounts of email, and take steps to determine if the computer is acting as a spam zombie. When necessary, quarantine the affected computer until the source of the problem is removed.

- give your customers plain-language advice on how to prevent their computers from being infected by worms, trojans, or other malware that turn PCs into spam zombies, and provide the appropriate tools and assistance.

- provide, or point your customers to, easy-to-use tools to remove zombie code if their computers have been infected, and provide the appropriate assistance.

---

[1] If you implement these recommendations, please ensure that they do not conflict with any existing laws in your jurisdiction, such as data protection, privacy or information security laws, or other legal requirements or obligations. Note also that these recommendations may already be mandatory in some jurisdictions.

Finally, in addition to encouraging ISPs to prevent spammers from creating zombie computers, we are developing a plan for identifying the IP numbers of likely spam zombies around the world, as well as the ISPs and other providers of Internet connectivity that appear to be responsible for the affected IP numbers. That analysis will be based on publicly compiled information such as spam databases and WHOIS databases. We plan to contact those providers of Internet connectivity associated with IP numbers used by possible spam zombies. This second letter will request that the affected providers step up their efforts to fight apparent spam zombie problems on their systems.

For more information about this project, and to see a list of the agencies partnering in this effort, visit www.ftc.gov/bcp/conline/edcams/spam/zombie/index.htm.

Thank you for your assistance in the fight against spam.