Design and Implementation of a Proxy Emulator to Capture Spam in Low Interaction Honeypots

Klaus Steding-Jessen\textsuperscript{1,3}, Antonio Montes\textsuperscript{2,3}, Nandamudi L. Vijaykumar\textsuperscript{3}

\textsuperscript{1}Computer Emergency Response Team Brazil – CERT.br
Brazilian Internet Steering Committee – CGI.br
\textsuperscript{2}Renato Archer Research Center – CenPRA
Ministry of Science and Technology – MCT
\textsuperscript{3}Computing and Applied Mathematics Laboratory – LAC
Brazilian National Institute for Space Research – INPE

\texttt{jessen@cert.br, antonio.montes@cenpra.gov.br, vijay@lac.inpe.br}

Keywords: honeypot, proxy, SOCKS, spam.

Spam is one of the Internet abusive activities that have most increased in the past few years. Today it is responsible for a significant part of the e-mail circulating on the Internet (Hayes 2003). It has also being used as a vehicle to send phishing and to disseminate malicious code (Milletary 2005).

The term spam is used to describe the act of sending unsolicited messages indiscriminately, specially in large quantities and with commercial purpose (Shirey 2000, Hambridge & Lunde 1999).

There is a lack of precise data about the impact and the mechanisms used for the dissemination of spam and malicious code. This is one of the current problems for the creation of effective mechanisms to mitigate the problem.

This work presents the design and implementation of a SOCKS (Leech, Ganis, Lee, Kuris, Koblas & Jones 1996) proxy emulator for low interaction honeypots, to be used for spam capture and study.

A proxy server acts as an intermediary program, making requests on behalf of other clients (Fielding, Gettys, Mogul, Frystyk, Masinter, Leach & Berners-Lee 1999). When it allows indiscriminate connections from any clients, it is called an open proxy. Spammers use open proxies to connect to their victims SMTP servers in order to remain anonymous (Chuvakin 2003). Open proxies are the result of poorly configured programs or are installed by bots and other malicious software.

In this work we developed a module designed to emulate the behaviour of an SOCKS open proxy in order to capture spam. This module was designed to work with the low interaction honeypot Honeyd (Provos 2004).

The module implements the SOCKS (Leech et al. 1996) protocol versions 4 and 5, and is configured to listen on ports usually used by this protocol, like 1080/TCP, 10080/TCP, etc. The spammer usually connects to the proxy to redirect its connection to the IP address of the victim’s SMTP server, on port 25/TCP. The proxy emulator then redirects the connection to a local SMTP server, giving a SMTP banner similar to that of the victim. Once the spammer believes the connection was succesfull he starts delivering
the messages. At this point, the emulator starts to capture all the spam messages, and store them in the honeypot for further studies.

References


