HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

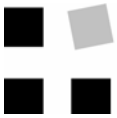
Kurzfassung 2. Semesterarbeit

Abteilung	**Informatik**
Namen	**Roger Britt** **Marc Bechtiger**
Semester	**SS06**
Titel der Semesterarbeit	**Botnet Detektion mit Snort**
Examinatorin / Examinator	**Prof. Dr. P. Heinzmann**

Das Projekt zur Detektion von Bot-verseuchten Rechnern und Botnet-Servern wurde Anfang 2005 durch Prof. Dr. P. Heinzmann von der cnlab AG initiiert. Nach Vorstudien Ende 2005 realisierten nun die Studenten R. Britt und M. Bechtiger im Rahmen ihrer Studienarbeit an der HSR zwischen Februar und Juli 2006 ein Botnet Server Detektionssystem (bsd).

Bsd kann einerseits Botnet-Aktivitäten visualisieren und statistisch auswerten, andererseits dient bsd dazu, Botnetserver aufzuspüren und unterstützt so Internet Service Provider bei der Detektion und Säuberung von "botverseuchten" Rechnern. Die Detektion basiert auf der Überwachung des gesamten Verkehrs zwischen speziell konfigurierten Honeypot-Rechnern und dem Internet. Sendet der Honeypot-Rechner Datenpakete, welche auf eigens definierte Snortregeln zutreffen, so werden die Paketfolgen in eine Datenbank geschrieben und automatisch ausgewertet. Den aufgezeichneten Paketfolgen ordnet die bsd-Software Events, wie beispielsweise DNS-Query/-Response, IRC-Kommunikation oder TFTP-Downloads zu. Solche Events werden graphisch dargestellt und nach verschiedenen Kriterien ausgewertet. Die Erfassung, Steuerung und Überwachung des gesamten Messablaufs ist als Webanwendung realisiert.

Erste Tests zeigen, dass sich beispielsweise am Cablecom-Breitbandnetz Botnet-Server ca. im 5min Takt detektieren lassen. Es ist eine beachtliche Liste von aktiven Botnet-Servern - es waren rund vierzig neue Botnet-Server, bei gut 1000 gefangenen Bots, pro Woche - zustande gekommen. In der Testphase wurde aber auch beobachtet, dass in gewissen Situationen plötzlich keine Bots mehr den Honeypot besuchten oder dass bei einem anderen Internet-Provider überhaupt keine Bots „gefangen“ werden konnten. Bsd soll nun eingesetzt werden, um umfangreichere Botnet-Server-Listen zu erstellen und um die Botnet-Arbeitsweisen besser zu verstehen. Dabei sollen auch die Gründe für die beobachteten „Aussetzer-Effekte“ und ISP-Unterschiede gefunden werden.



HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL