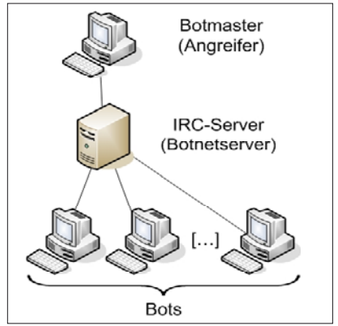
Botnet Pandemie?

Stefan Graf
Andreas Wüst

Diplomanden	Stefan Graf, Andreas Wüst
Examinator	Prof. Dr. Peter Heinzmann
Experte	Dr. Thomas Siegenthaler, CSI Consulting AG
Themengebiet	Internet Security
Projektpartner	Dr. R. Halbheer, Microsoft Schweiz GmbH



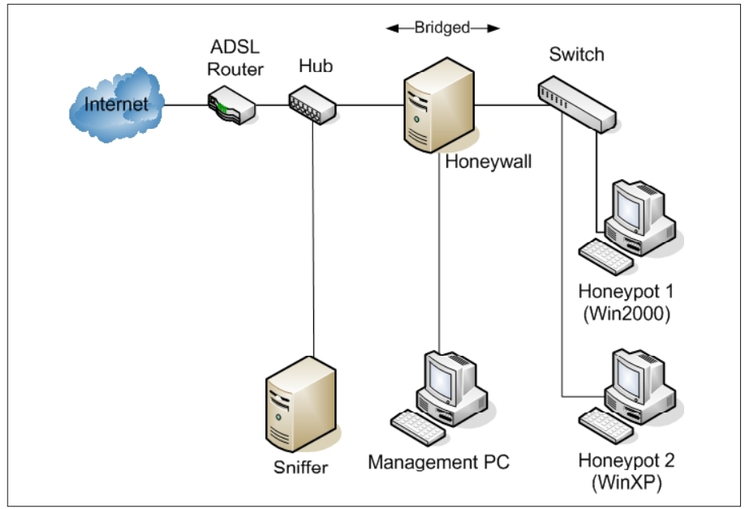
Aufbau eines Botnet

Aufgabenstellung: Die Verbreitung von fernsteuerbaren versteckten Programmen – so genannten Bots – auf Internet Rechnern wird zunehmend zum Problem: In einem Botnet kooperierende Bots werden von einem Botmaster aus über Internet-Relay-Chat (IRC) gesteuert. Sie spionieren Privatrechner aus (sammeln Passwörter und Kreditkartennummern), versenden SPAM Mails oder nehmen an Denial-of-Service-Attacken teil. Damit beeinträchtigen Bots nicht nur die Nutzbarkeit der Rechner, sondern auch die Verfügbarkeit von Internet-Service-Provider (ISP) Diensten (z.B. von Mail).

Daher soll eine Plattform zur Analyse von Botnet-Aktivitäten realisiert werden, welche hilft, infizierte Rechner eines Providers zu finden und zu säubern. Es soll auch möglich sein, die Bot-Situation bei Schweizer ISP zu vergleichen.

Ziel der Arbeit:

- Beschreibung der Botnet Funktionsweisen und Beurteilung von Ansätzen zur Bot-Detektion
- Aussagen über die Bot-Situation bei Schweizer Internet Service Providern
- Konzept zur Identifikation von mit Bots infizierten Rechnern



Versuchsaufbau des Honeynet

Lösung: Es wurde ein System zum «Einfangen» von Bots aufgebaut. Dieses so genannte Honeynet umfasst «Opferrechner» (Honeypots) und Kontrollsysteme (Honeywall, Sniffer, Mgmt PC). Basierend auf der systematischen Analyse der Kommunikation von «gefangenen» Bots mit ihrem Botnet-Server wird ein Konzept zur Identifikation von mit Bots infizierten Rechnern vorgeschlagen:
Aus der Analyse des Botnet-Verkehrs werden «Botnet-Signaturen» gewonnen. So können Internet Service Provider (ISP) den Datenstrom ihrer Kunden nach diesen Signaturen absuchen und mit hoher Wahrscheinlichkeit bestimmen, welche Rechner Teil eines Botnets sind.
Im Rahmen der Tests mit dem realisierten Honeynet werden Daten zu Botnet-Aktivitäten bei verschiedenen Schweizer ISP gesammelt. Damit sollten nach dem Abschluss der Arbeit Aussagen zu Unterschieden bei Schweizer ISP möglich sein.