Technische Universität München
Lehrstuhl für Netzarchitekturen & Netzdienste
Prof. Dr. Georg Carle

13.07.2009

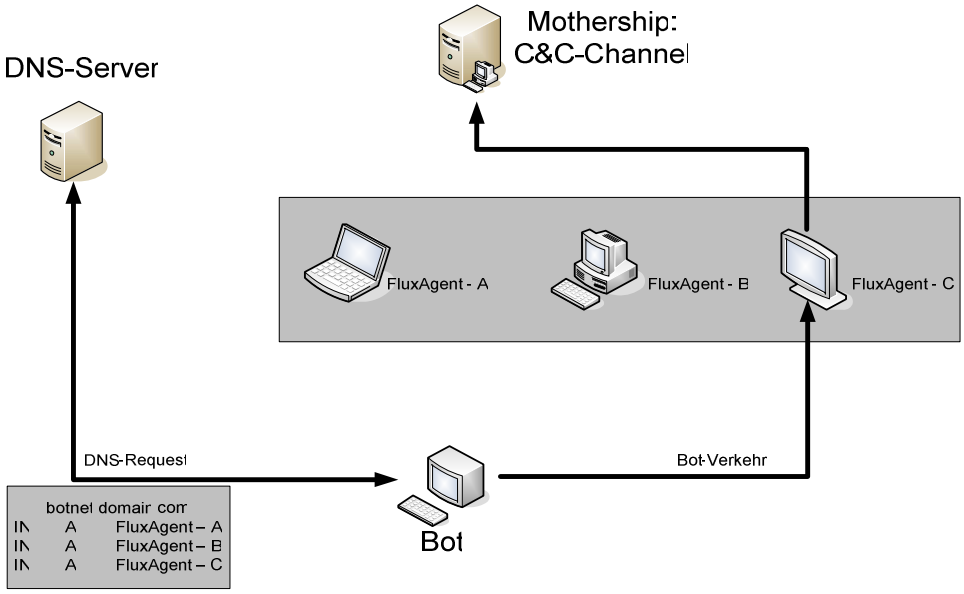
Diplom-/ Bachelor-/ Masterarbeit/SEP

Untersuchung von Fast-Flux-Netzwerken

Beschreibung

Viele Botnetze werden mit Hilfe eines zentralen Servers kontrolliert. Z. B. können über IRC- oder HTTP-Server Befehle an Bot-Clients ausgegeben werden. Die dafür notwendige Infrastruktur ist einfach aufzusetzen. Jedoch hat sie für den Botmaster einen entscheidenden Nachteil: Die IP-Adresse und damit der Standort des Systems können über DNS-Einträge leicht identifiziert werden. Der Server kann somit leicht geblockt oder vom Netz genommen werden, wodurch das Botnetz für den Botmaster verloren ist.

Um dies zu umgehen werden heute von Botmastern verstärkt *Fast-Flux-Netzwerke* eingesetzt. Diese verschleiern den Standort des Servers indem sie *Flux-Agents* unter dem DNS-Namen des Botnetzwerkes bekannt machen. Die *Flux-Agents* fungieren als Proxy und reichen Anfragen an den Server, das sogenannte Mothership, weiter und verstecken es damit. Wird einer der *Flux-Agents* vom Netz genommen, kann das Botnetz mit Hilfe der anderen *Flux-Agents* weiter operieren.



Aufgabenstellung

Fast-Flux-Netzwerke unterscheiden sich durch verschiedene Eigenschaften von anderen Domains. Im Rahmen der Arbeit sollen verschiedene Methoden zur Erkennung von *Fast-Flux-Domains* implementiert werden. Mit Hilfe der Implementierungen sollen aktive *Fast-Flux-Domains* identifiziert, beobachtet und untersucht werden.

Infos & Kontakt

Lothar Braun, braun@net.in.tum.de Tel.: 289-18010