

## **DDOS-Angriffe mittels Botnets**

Autoren: Sebastian Schreiber, Stefan Arbeiter

Dieses Jahr wurde zum ersten Mal öffentlich bekannt, das sogenannte D.D.o.S.-Angriffe mit erpresserischen Zielen durchgeführt wurden, auch wurden die ersten Erfolge von Strafverfolgungsbehörden in England gegen Täter gemeldet - was steckt aber dahinter?

Die Angriffstechniken selbst sind seit langem bekannt: Die grundlegende Funktionalität der im Internet eingesetzten Protokolle wird verwendet um ein oder mehrere Zielsysteme lahmzulegen.

In der einfachsten Variante wird nur durch zahlreiche HTTP-Anfragen versucht, die Kapazitäten der Zielseite vollständig auszulasten, wobei unerheblich ist, ob der Zielsever die Anfragen nicht mehr bearbeiten oder die gesamte Bandbreite verbraucht wird: Resultat ist, das der Zugriff legitimer Besucher quälend langsam oder unmöglich wird. Eine weitere, alltägliche Variante ist die SYN-Flood, bei der versucht wird, durch unvollständige TCP-Drei-Wege-Handshakes das Zielsystem unereichbar zu machen.

Eine bedrohliche Schlagkraft entfalten solche Angriffe natürlich erst, wenn sie selbst genügend Last erzeugen können, daher bietet sich die Koordination von sehr vielen Systemen mit guter Anbindung an, es wurde schon bekannt, das solche Angriffsnetze aus bis zu 10000 Rechnern bestehen können.

Interessant sind vor allem die Techniken, die verwendet werden, um die Rückverfolgung eines solchen Angriffes zu verschleiern.

Bei halbwegs professionellen oder paranoiden Tätern wird nicht der eigenen PC direkt für einen solchen Angriff bzw. seine Koordination verwendet. Der Angreifer verwendet statt dessen bestenfalls einen Pool gehackter Systeme, von denen er weiss, dass seine Aktivitäten nicht weiter beachtet werden.

Bezüglich der Steuerung des Angriffes ist auch in diesem Bereich eine erhebliche Verbesserung erzielt worden: Stacheldraht, dem ein einfaches Client-Server Modell zu Grunde lag, verlangte von den Betreibern noch, den Client, das eigentliche Angriffswerkzeug, manuell zu installieren oder einen "Mass-Router" zu verwenden. Eine Software, die ein oder mehrere Sicherheitslücken ausnutzen konnte, um den Client zu verteilen.

Auf ausgewählten Systemen wurde dann das Kontroll-Programm (Master) gestartet, um den Clients Kommandos, meist getarnt als DNS-Verkehr zu geben. Das Opfer eines Angriffes kennt im ersten Schritt nur die Clientsysteme, und musste zumindest einen Betreiber erreichen, um auf legalen Wegen die Systeme mit Kontrollprogrammen zu finden.

Als weiteres System für die Client-Steuerung hat sich IRC stark etabliert: Die Möglichkeit, in diesem Chatsystem automatische User (Bots) zu verwenden, wurde in die Clientsoftware, ob sie nun als Trojaner und/oder Wurm verbreitet wird, integriert, daher der Name Botnet. Jedes mit dem "Bot" infizierte System nimmt Kontakt mit einem IRC-Server auf, und meldet sich dort wie ein regulärer User an. In dem von den Bots verwendeten Kanal können dann einfache Steuerkommandos an die infizierten Systeme weiterzugeben, um Ziele anzugreifen oder sich selbst upzudaten, wenn der Angreifer die Funktionalität erweitert hat. Botnets und deren Angriffe sind ein Problem mit denen IRC-Netze schon lange zu kämpfen haben.

Zwar mag der Aufbau eines Botnets unauffällig sein, sobald es aber zum Angriff eingesetzt wird, werden die einzelne infizierte Systeme (Auch "Zombies" genannt) sofort erkannt: Der Betreiber einer Serverfarm im Internet wird schnell merken, das seine Systeme Teil eines Botnets geworden sind, aber was ist mit dem Privatanwender, dessen PC DSL-Zugang zum Internet hat? Eventuell fällt ihm der zusätzliche Verkehr erst dann auf, wenn er die Leitung blockiert. Tatsächlich bestehen botnets heute immer mehr aus infizierten Maschinen von Heimanwendern, die schlecht oder garnicht gewartet werden.

Der Umgang mit Bot-Infektionen ist letztlich derselbe wie mit jeden Wurm: Infizierte Maschinen müssen vom Netz genommen und so schnell wie möglich gereinigt werden. Für das Opfer eines Botnet-Angriff wiederum hilft nur perfekte Koordination mit dem ISP, um den Verkehr, den das Netz erzeugt, geschickt zu blockieren. Da es sich um zahlreiche Systeme handelt, zwischen denen keinerlei regionale Verknüpfung besteht, ist diese Aufgabe nicht trivial - es ist daher nicht verwunderlich, dass die Angriffe zumindest zeitweise Erfolg haben.

Schockierend ist der Preis, für den ein Botnet zu haben ist: der Admin Andrew Kirch berichtet in einem Interview auf Newsforge, das ein Netz aus mehreren Bots für den lächerlichen Preis von 500 US Dollar den Besitzer gewechselt hat.