

## newsletter

# zum Thema **Botnets** Sicherheitsbedrohung im Internet

**Botnets sind eine relativ neue Entwicklung im Bereich der Internetkriminalität. Experten zählen sie zu den größten Sicherheitsbedrohungen bei der Nutzung des Internets. Mittels Botnets ausgeübte Attacken sind zielgerichtet und meist darauf ausgelegt, vertrauliche Informationen zu erhalten oder die Opfer finanziell zu schädigen.**

### **Begriffs- erklärung**

Botnet ist die Abkürzung des Begriffs Roboter-Netzwerk. Es handelt sich dabei um ein fernsteuerbares Netzwerk von Computern, die über das Internet verbunden sind. Auf dem einzelnen, zum Bot-Netz gehörenden Computer ist mittels Viren bzw. Trojanern - meist ohne das Wissen des Nutzers - ein Stück Software eingeschleust worden. Mittels dieser Software wird das System von außen kontrollierbar.

Ursächlich für die Infektion der einzelnen Rechner sind meistens fehlende Sicherheits-Updates und ein nicht aktueller Virenschutz.

Systeme (Rechner), die über Bot-Netze zusammen geschlossen sind, werden auch als „Zombies“ bezeichnet. Die im Bot-Netzwerk zusammengeschlossenen Rechner werden zentral kontrolliert und können für diverse cyberkriminelle Aktivitäten eingesetzt werden.

Ein Botnet setzt sich typischerweise aus mehreren hundert oder tausend Rechnern zusammen, wobei auch Netzwerke beobachtet wurden, die sogar hunderttausende von Zombie-Rechnern kontrollieren. Derartig große Botnets verfügen über eine ausreichend große Zahl von Zombie-Rechnern, so dass sie Server mit einer Datenlast von mehreren hundert Mbit pro Sekunde bombardieren können. Ein derartig massiver Datenstrom kann selbst großen Internet Service Providern erhebliche Probleme bereiten.

### **Hintergrund**

Anfang Februar 2007 wurden die für die Kommunikation über das Internet essentiellen Root-Name-Server des Domain-Name-Systems (DNS) Ziel einer großangelegten Attacke. Derartige über Botnets ausgeführte Attacken stellen schon seit einigen Jahren insbesondere für im Internet tätige Unternehmen ein ernst zu nehmendes Bedrohungspotenzial dar. Immer häufiger werden Netzbetreiber und Internet Service Provider zum Angriffsziel von Bot-Netzwerken, die mittels koordinierter Attacken in der Lage sind, ganze Servernetze lahm zu legen. 2005 wurden in den Niederlanden mehrere Personen verhaftet, die ein Bot-Netzwerk mit ca. 1,5 Millionen Rechnern aufgebaut hatten mit der Absicht, unter Androhung von Denial of Service Attacken Unternehmen in den USA zu erpressen. Mitte 2004 legte beispielsweise eine Botnet-Attacke auf das Servernetz des Webhosters Akamai die Web-Sites von Apple, Google, Microsoft und Yahoo für mehr als zwei Stunden lahm.

Bot-Netzwerke können als „Allzweckwerkzeuge“ der Computerkriminalität sehr vielseitig für illegale Machenschaften eingesetzt werden. Zudem werden Botnets von ihren Besitzern gegen Gebühr an andere Kriminelle vermietet.

## Einsatzmöglichkeiten von Botnets

Zu den häufigsten Einsatzmöglichkeiten zählen:

- Denial-of-Service-Angriff: Denial-of-Service-Attacken im Internet gibt es bereits seit vielen Jahren. Denial of Service (= den Dienst verweigern) bezeichnet einen Prozess, der darauf abzielt, Netzwerkdienste (z. B. einen Web- oder Mailserver) lahmzulegen. Dabei wird die Netzanbindung des Angriffsziels mit einer großen Anzahl von Datenpaketen überflutet, was letztendlich zu einer Überlastung und u. U. zum Absturz des Systems führt. Die dazu notwendige Datenlast wird mit Hilfe eines Botnets erzeugt.  
*(siehe: Distributed Denial of Service Attacken im Internet, AssTech newsletter 2002).*
- Erpressung: Im Internet tätigen Unternehmen wie Internet Service Providern, Online-Diensten oder E-commerce-Anbietern wird eine Denial-of-Service-Attacke angedroht, die ihr System lahm legt, sofern nicht ein bestimmtes Löse-/Schutzgeld bezahlt wird.
- Spam: Botnets sind in der heutigen Spam-Industrie von zentraler Bedeutung. Da durch den Einsatz von Botnets die Spam-E-Mails von vielen verschiedenen (Zombie)Rechnern verschickt werden, sind die tatsächlichen Absender dieser E-Mails nur sehr schwer ausfindig zu machen.
- "Phishing": Für Phishing-Attacken werden Botnets sehr häufig eingesetzt: Sowohl zur Versendung der betrügerischen Phishing-Mails als auch beim Hosting der dazu verwendeten illegalen Websites.  
*(siehe: Phishing – Sicherheitsbedrohung im Internet, AssTech newsletter 2005).*

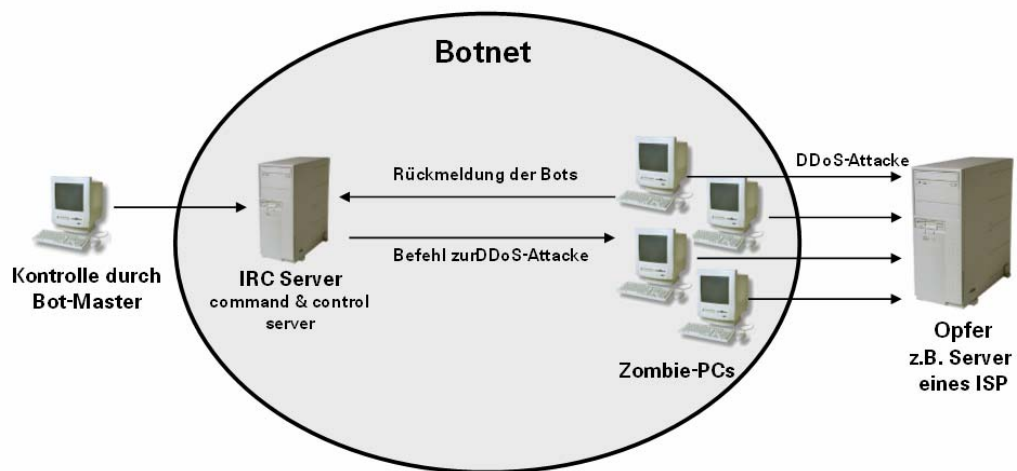


Abbildung: Aufbau eines typischen Botnets mit einem zentralen Internet-Relay-Chat-Server, der durch einen sog. Bot-Master kontrolliert wird. Als Beispiel greifen die Zombies des Botnets hier einen Server mittels einer Distributed Denial of Service Attacke an.

## Fazit

Botnets stellen derzeit ein zentrales Element im Rahmen der Cyberkriminalität dar. Durch zielgerichtete Angriffe bzw. deren Androhung veranschaulichen sie den gegenwärtigen Trend, weg vom Hacker als Einzeltäter hin zu gut organisierten kriminellen Angreifer-Gruppen.

Gerade für eine in immer stärkerem Maß vernetzte und digitalisierte Weltwirtschaft, die zunehmend von der Verfügbarkeit von IT- Systemen abhängt, stellen

Botnets allein schon auf Grund ihrer Größe und der Tatsache, dass die Hintermänner nur schwer zu ermitteln sind, eine ernst zu nehmende Bedrohung dar.

Insbesondere die über Botnets ausgeführten DDoS-Attacken (DDoS = Distributed Denial of Service) bedeuten eine zunehmende Gefahr für Unternehmen, deren Geschäftstätigkeit in hohem Maß auf einer Präsenz im Internet basiert. Bisher wurde vornehmlich versucht, bestimmte E-Commerce-Anbieter und -Institutionen mittels dieser Angriffstechnik lahmzulegen. Ein wesentlich massiveres Bedrohungsszenario jedoch stellen gezielte Angriffe auf die Kernelemente der Infrastruktur des Internets mit einem großflächigen wirtschaftlichen Schadenszenario dar.

#### **Hinweise für das Underwriting**

Insgesamt betrachtet ist das Schadenpotenzial durch Botnets nur schwer abschätzbar, da viele Attacken von Unternehmen aus Imagegründen nicht publik gemacht werden. Auf Grund ihrer sehr großen „Angriffsressource“, können über Botnets ausgeführte Attacken selbst für größere im Internet tätige Unternehmen ein gravierendes Risiko darstellen.

Die durch Bot-Netzwerke verursachten Ausfälle von IT-Systemen, z.B. durch Denial of Service-Attacken, entstehenden Vermögensschäden sind typischerweise in Standard-Sach- und Haftpflichtdeckungen nicht versichert. Für derartige Szenarien existieren spezielle Versicherungsprodukte, die in begrenztem Umfang spezifisch IT- und Internetrisiken inkl. Netzausfälle decken.

Ungenügender Schutz von IT-Systemen gegen unbefugten Zugriff schafft die Möglichkeit, solche Systeme als Angriffswerkzeuge (Zombies) zur Schädigung Dritter zu missbrauchen. Dies kann grundsätzlich Haftungsansprüche der Geschädigten gegen die Betreiber der missbrauchten Systeme zur Folge haben.

Eine auf Grund einer Botnet-Attacke hervorgerufene Betriebsunterbrechung, beispielsweise durch den Ausfall externer Netzwerke, kann zu entsprechenden Rückwirkungsschäden (suppliers /customer extension) führen. Auch hier kommt der Risikoprüfung eine hohe Bedeutung zu, speziell im Hinblick auf Schnittstellen und Abhängigkeiten zu Internet Service Providern, Hostern und Carriern. Bei Versicherungskonzepten, die Betriebsunterbrechungen bei IT-Systemen ohne zugrundeliegenden Sachsubstanzschaden decken, ist eine Kumulexposure auf Grund von Angriffen auf die Internet-Infrastruktur gegeben, insbesondere im Hinblick auf den Ausfall von zentralen Infrastrukturelementen. Dieses Kumulschadenszenario ist äußerst schwierig zu kontrollieren.

#### **Kontakt**

AssTech GmbH  
Postfach 1211  
85766 Unterföhring bei München  
Telefon + 49 89 3844-1585  
Telefax + 49 89 3844-1586  
info@asstech.com  
www.asstech.com