

DDoS – Distributed Denial of Service

© & written 2003 by M.Rogge & Mixer

Diese Art der Angriffsform auf ein Netzwerk oder einzelnen Computer ist derzeit nach wie vor eine der gefährlichsten Formen die es gibt.

DDoS Angriffe legen meistens einen ganzen Host, der zumindest auf TCP/IP basiert, für mehrere Stunden lahm.

Oftmals werden ganze Hosts oder IP Ranges davon betroffen, sodass diverse Services nicht mehr erreichbar sind.

Zweifelsohne kann man davon ausgehen, dass dies kein Machwerk eines Crackers ist, der sich „probieren“ will, sondern immer eine böswillige Absicht mit einer solchen Attacke verfolgt wird. (Angriff)

Der Erfolg einer DDoS Attacke ergibt sich aus der Struktur dieser Angriffsform, da diese verschiedene Rechnerkapazitäten verwenden und verteilt arbeiten, um dann einen gemeinsamen „Schlag“ gegen den betreffenden Host auszuführen.

Verschiedene Formen sind hier möglich nach denen eine solche Attacke aufgebaut sein kann.

Die Angriffsformen einer DDoS Attacke:

Zum einen können gespoofte ICMP Echo Request Pakete an den betreffenden Host gesendet werden der dann aber nach gewisser Zeit bei einer Übermenge an Antworten die Arbeit niederlegt und sich abschaltet.

Über TCP Pakete ist es teilweise möglich eine bestimmte Menge TCP Pakete an den Zielhost zu senden, diese werden aber bei 50% wieder abgebrochen und der Zielhost bricht nach kurzer Zeit zusammen und kann nicht mehr arbeiten.

Die effektivsten DDoS Programme existieren derzeit nur unter der Arbeitsplattform Linux/Unix. Tools die für Windows angeboten werden überlasten oftmals das System von Windows selbst, da die Schnittstelle von Windows dahingehend nicht die stabilste ist.

DDoS Angriffe können sich gegen einen entfernten Host, eine Hardware oder gar gegen bestimmte Software richten.

(z.B. Real Audioplayer, MS Windwos 98/2000/NT4/XP, Cisco-Router)

Eines der DDoS Programme die derzeit am effektivsten arbeiten ist **TFN 2000**.

TFN = Tribe Flood Network 2000. (kurz TFN2k)

Das von Mixer programmierte Tool bietet verschiedene Möglichkeiten in einem Programm der Distributed Denial of Service Attacken.

Ich schildere Ihnen die genaue Arbeitsweise des Programmes TFN2k, die Vorteile, Nachteile und die Gegenmaßnahmen, die ergriffen werden können.

Bei konventionellen DoS Angriffen, die auf Flooding, d.h.der Überlastung der maximalen Bandbreitenkapazität eines Ziels basieren, muss einem Angreifer immer ein System zur Verfügung stehen, dass über wesentlich mehr Bandbreite als sein Ziel verfügt, damit das Ziel mit kontinuierlichen Anfragen überlastet werden kann.

Wenn nicht, dann muss ein Angreifer auf mehrere Systeme mit geringerer Bandbreite zurückgreifen, um so einen Angriff zu koordinieren - also etwa in dem er sich über etliche Telnet- oder SSH-Sitzungen einloggt und gleichzeitig einen Pingbefehl ausführt - dessen Gesamtbandbreite dann wieder die Bandbreite des Zielsystems wesentlich übersteigt.

Verteilte DoS-Angriffe automatisieren dieses Schema, indem sie auf simpler Client/Server Technologie aufbauen.

Ein DDoS-Server oder DDoS-Daemon wartet auf Anweisungen, Ziele anzugreifen, also kontinuierlich Daten an ein Ziel zu senden.

Diese Anweisungen werden in einem für das DDoS-Programm anwendungsspezifischen Protokoll übertragen.

Ein DDoS-Client, welcher dasselbe Kontroll-Protokoll unterstützt, wird benutzt, um Angriffsanweisungen für ein Ziel an beliebig viele DDoS-Server zu schicken, und somit Angriffe zu koordinieren.

Besonderheiten der TFN2k-Technologie:

Bei anderen DDoS-Applikationen halten DDoS-Server ständig Verbindungen mit dem DDoS-Client offen.

Der Client wird zu einer Art Hub oder Master-Server, der mit allen Servern verbunden ist. TFN2k dagegen benutzt keine Verbindungen.

TFN2k benutzt ein proprietäres Protokoll, um Kontroll-Anfragen an seine DDoS-Server zu verschicken.

Das Protokoll selbst ist zwar simpel, aber trotzdem sicher genug, um nicht einfach erkannt zu werden.

Es setzt sich über die Internet-Standards TCP, UDP und ICMP hinweg: es benutzt im Zufallsverfahren eines dieser Protokolle, und hängt die relevanten Daten als Payload eines TCP-UDP- oder ICMP-Paketes an.

Die Kontrolldaten enthalten die Art des Angriffs (oder andere Funktionen wie Fernzugriff, verteilte Befehlsausführung, Angriffsende, usw.) und eine Liste von Zielsystemen.

Diese Daten sind mit CAST256, einem symmetrischen Algorithmus, verschlüsselt, und in BASE64 kodiert.

Wichtig ist hier, dass diese Pakete nicht von normal vorkommenden Datenpaketen zu unterscheiden sind, und auch dass so keine Verbindung hergestellt werden muss.

Anders als bei einer Verbindung gehen die Pakete, und die enthaltenen Nachrichten in eine Richtung -- nur vom DDoS-Client zu den jeweiligen DDoS-Servern.

Darüberhinaus sind sämtliche Absenderadressen der Kontrollpakete gespoofed, d.h. es werden einfach beliebige Absender im Quell-IP-Feld eingetragen.

Symmetrische Verschlüsselung ist eine wirkungsvolle Waffe gegen jede Art von Systemen zur Erkennung z.B. von DDoS-Kontroll-Datenverkehr.

Es findet kein Austausch von Schlüsseln oder Authentifikation statt, daher ist der gesamte Inhalt der Kommunikation verschlüsselt und nicht nachvollziehbar.

Bei DDoS-Netzwerken ist symmetrische Verschlüsselung möglich, weil es sich um "private" Netzwerke handelt: alle DDoS-Server und der DDoS-Client werden vom selben Nutzer installiert, verfügen also über denselben geheimen symmetrischen Schlüssel.

DDoS-Funktionalität:

Es gibt mehrere Arten von Angriffen, die koordiniert werden können, darunter UDP (Bandbreitenüberlastung durch UDP-Pakete, und ICMP-Fehlermeldungen, die vom Angriffsziel generiert werden, wenn ein UDP-Paket auf einen geschlossenen Port trifft), durch ICMP-Pakete (Ping-Anfragen die entsprechend Ping-Antworten generieren), sowie TCP/SYN-Angriffe (permanente Anfragen von zufälligen Quelladressen, neue TCP Verbindungen aufzubauen, was nicht nur die Bandbreite sondern auch die Ressourcen von Serverprogrammen, etwa eines Apache Webservers, sowie von Betriebssystemen überlastet).

Darüberhinaus bietet TFN2k die verteilte "**Targa3**"-Attacke.

Hierbei handelt es sich um Pakete, die mit zufälligen Werten erstellt werden.

Es kann sich also um UDP, ICMP, IGMP, TCP, oder andere Protokolle handeln, um Fragmente, oder nach den Protokollstandards völlig ungültige Pakete.

Dies stellt eine Herausforderung für die Implementation des Netzwerksystems vieler Betriebssysteme dar, die nicht alle Sonderfälle von ungültigen Datenpaketen ohne weiteres verarbeiten können.

Zu den weiteren "Features" von TFN2k zählen Decoy-Pakete, also falsche "Dummies", die zusätzlich zu den echten verschickt werden können, um eine Entdeckung des Traffics zusätzlich zu erschweren.

TFN2k ist darüber hinaus Multi-Platform-fähig, läuft also auf den meisten gängigen Betriebssystemen.

Das bedeutet, es wäre möglich, DDoS-Server auf Linux, Solaris, BSD und Windows NT Systemen zu installieren, und Angriffe von all diesen Systemen gleichzeitig zu koordinieren.

Schwächen und Gegenmassnahmen:

Die Schwächen von TFN2k bestehen zum einen darin, dass es sich vom Konzept her darauf verlässt, dass IP-Spoofing, also das Fälschen von Absenderadressen, problemlos möglich ist. Auf diesem Vorgang beruht die Anonymität der Kontroll-Anfragen sowie der eigentlichen Angriffe in Form gespoofter UDP, TCP oder ICMP-Floods.

Implementiert ein Netzwerk, auf dem ein DDoS-Server oder DDoS-Client eingesetzt wird, das sogenannte "Ingress Filtering" zum Schutz gegen falsche Absenderadressen, so wird es einem Angreifer unmöglich sein, TFN2k anonym dort einzusetzen.

Eine weitere Schwäche besteht in der Implementation der Verschlüsselung: BASE64 (auch z.B. "Ascii-Armoring" bei PGP genannt), das verwendet wird, lässt sich, wenn auch mit etwas Aufwand, von anderen Paketen unterscheiden, da es nur aus alphanumerischen Zeichen besteht.

Dies ist aber eine implementationsspezifische Schwäche bei TFN2k, keine Konzeptionelle; die gleiche DDoS-Funktionalität könnte auch bei binärer Verschlüsselung realisiert werden.

Beispiel:

Ein Angreifer wird TFN2k kompilieren und dabei sein eigenes geheimes Verschlüsselungs- und Autorisierungs-Passworts (für Client und Server das selbe) zu wählen.

Ihm steht ein Serverprogramm ("td") zur Verfügung, daß auf einer Reihe von Systemen, die zum Angriff bereit sein sollen, mit root-Rechten installiert wird.

Der Server selbst wird auch versuchen, seine Existenz in der Prozesstabelle, durch einen harmlos erscheinenden Namen wie "httpd" oder "-bash", zu verstecken.

Die IP-Adressen sämtlicher DDoS-Server trägt der Angreifer in eine Textdatei (im Beispiel "servers.txt") ein.

Um anonym zu befehlen, das Ziel 192.168.1.23 mit ICMP-Anfragen anzugreifen, muss ein Angreifer lediglich den folgenden Befehl geben:

```
tfn -f servers.txt -c3 -i 192.168.1.23.
```

Hiermit kontaktiert der Angreifer alle DDoS-Server aus "servers.txt", die dann ihrerseits das Ziel, 192.168.1.23, koordiniert mit Typ 3 (ICMP) angreifen werden.

Der Angriff kann mit -c0 wieder beendet werden.

TFN2k kann kurz gesagt von einem Attacker sehr gezielt auf ein Netzwerk wirkungsvoll eingesetzt werden, da der Attacker gleichzeitig mehrere Clients bedienen kann.

Die Clients kommunizieren bei TFNk2 über ICMP Pakete und nicht wie herkömmliche Angriffstools über einen Port.

Die Clients geben die Datenpakete an die Daemons weiter, die dann das anzugreifende Zielsystem attackieren.

(Zielsystem oder auch Opfer oder Victim genannt)

Es steht nicht im Widerspruch dazu, daß mit Programmen wie TFN2k DDoS Attacken realisiert werden können sondern darauf aufmerksam gemacht werden soll, welche Schwächen bestehen und wie diese gesichert werden können.

Es gibt natürlich auch andere Programme, die auf einer anderen Struktur aufsetzen um ein Flood Netzwerk aufzubauen.

Vertretend und immer noch aktuell sind unter anderem Trinoo und Stacheldraht.

Auf beide DDoS Attackprogramme möchte ich an dieser Stelle kurz eingehen.

Trinoo oder Trin00

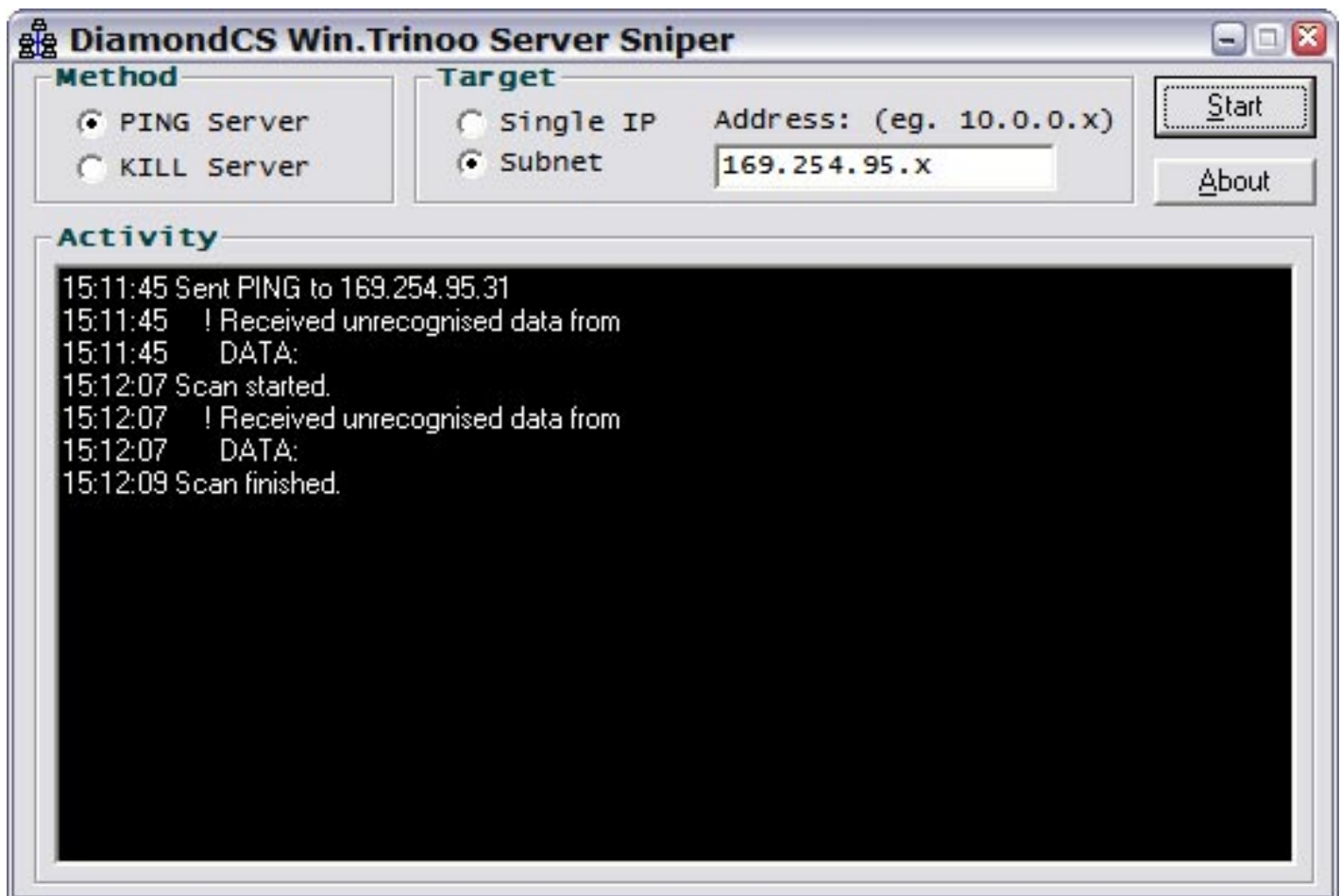
Trinoo besteht im wesentlichen aus einem Master den man als master.c vorfindet und einem Daemon, der meistens als ns.c zu finden ist.

Die Kommunikation bei Trinoo findet allerdings über Ports statt, nicht wie bei TFNk2, über Datenpakete.

Der Attacker gibt seine Befehle an die installierten Master über Port 27665 via TCP an. Die installierten Master senden ihre Befehle über UDP Port 27444 an den Daemon weiter und die Rückmeldungen vom Daemon an den Master läuft über UDP Port 31335. Wie auch bei TFNk2 ist es dem Attacker möglich, mehrere Master gleichzeitig zu bedienen. Die Master sind in diesem Fall jeweils als Server anzusehen, die vom Attacker gesteuert werden.

Ein Programm das Ihren Computer oder Server unter Windows auf Trin00 prüft gibt es von Diamond Computer Systems Pty. Ltd.

Nach der problemlosen Installation sollte der Computer neu gestartet werden, um so ein effektives Arbeiten mit dem Programm zu ermöglichen. Ist das Programm nun installiert, kann man es starten und die erforderliche IP eingeben, um den entsprechenden Host überprüfen zu lassen.



In unserem Beispiel haben wir zwei kurze Testläufe gemacht, die aber erfolgreich waren und kein Programm dieser Art gefunden wurde.

Das kleine Programm ist kostenlos und kann unter der folgenden URL auf den Computer geladen werden: <http://www.diamondcs.com.au/>

Stacheldraht

Stacheldraht hat eine leicht veränderte Arbeitsweise als Trinoo und TFNk2.

Bei Stacheldraht spricht man von einem Handler (mserv.c) der als Server fungiert.

Der Client (meist client.c) arbeitet als Element für die Verschlüsselung und Verbindung zwischen den Handlern.

Dies geschieht in der Regel bei der Kommunikation zwischen dem Client und Handler über TCP Port 16660.

Bei der Kommunikation zwischen dem Handler und den Agents sowie zurück wird TCP Port 65000 sowie ICMP echo reply angesprochen.

Der Attacker kommuniziert somit mit dem Client, der die Handler anspricht. Diese wiederum steuern die Agents und attackieren entsprechend das System/Opfer. (Victim)

Korrekturen: Udo Laumann, Mixer

Verweise und Downloads zum Thema:

[Mixer Security](#) - Homepage des Programmierers und Sicherheitsexperten

Download TFN2k: [Mirror Packetstorm](#)

Download TFN2k: [Brain-Pro Security](#)

Theoretischer Ausblick auf [Möglichkeiten von TFN3k](#)

DDoS Tools im Internet: [Packet Storm](#)

Download Trin00: [Brain-Pro Security](#)

Download Stacheldraht: [Brain-Pro Security](#)

Kurze Einführung in [TCP/IP & OSI Modell](#)

[DDoS](#), ein ausgezeichnetes Paper von Marc Ruef

[DDoS Software](#) von Computec

[Anti-Trin00 Sniper](#)

David Dittrich - [Analyse und Hintergrund zu TFN2k](#)

David Dittrich - [Analyse und Hintergrund zu Stacheldraht](#)

Bekannte DDoS Attacken: [Heise Newsticker vom 09.02.2000](#) und vom [10.02.2000](#)

Best Regards & Greetings

[Mixer](#) & [Marko Rogge](#)

Berichte dieser Seite sind in guter Absicht und mühsamer Arbeit erstellt worden, daher möchte ich Sie bitten keine Anleitung und/oder andere Texte frei zu kopieren.

Unter Angabe des Autors und der URL sowie eine Benachrichtigung per E-Mail ist eine weitere Veröffentlichung jederzeit möglich.

Für einen Missbrauch zeichnet sich der Autor nicht verantwortlich, da eine kriminelle Handlung oder vergleichbares Handeln nicht durch diesen Artikel unterstützt werden soll!

Sollte sich hier eine Information, Link, Bild oder dergleichen befinden das unerwünscht ist, bitte ich um eine kurze Nachricht an mich.

Ich werde diesen Mißstand umgehend korrigieren.