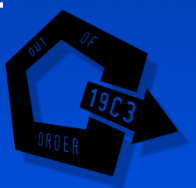
Detecting DDOS Attacks & Countermeasures at ISPs

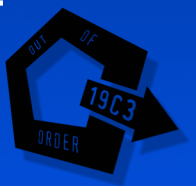
Jan-Ahrent Czmok

URL: www.lambda-solutions.de/ddos/
EMAIL:<czmok@lambda-solutions.de>
EMAIL:<czmok@gatel.de>



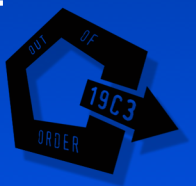
Intro

- Es geht um die Erstellung eines Kommunikationsforums zwischen der Community „Hacker“ und den ISPs um gemeinsam Lösungen für die DDOS-Problematik zu finden.
- Ergebnisse des Workshops werden bei einem der nächsten RIPE Meetings [1] vorgestellt.



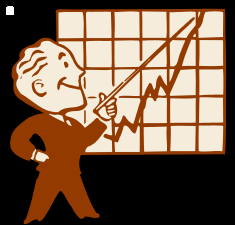
Thematik

- DDOS bedeutet eine Attacke von einen oder mehren Hosts gegen ein Ziel.
- Derzeit nur reaktive, aber nicht proaktive Reaktion möglich.
- Betroffen sind zunehmend Privatuser und „normale Websites“



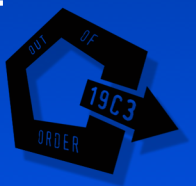
Thematik

- DDOS ist KEINE Belastung der Carrier, eher der ISPs, dem „Mittelstand“ in der Kette.
- Carrier-Awareness ist bis auf wenige Ausnahmen gering.
- ISPs sind sehr stark davon betroffen, da ihr Business davon abhängt, das die Anbindung funktioniert.



Art der Attacken

- DoS --smurf attacks (ICMP broadcast)
- DoS --fraggle attacks (e.g., UDP broacast to port 7)
- DoS --teardrop attack (IP fragmentation bugs)
- DoS --land attack (IP source = destination address)
- DoS --SYN flooding
- masquerading (TCP sequence number guessing)
- stealth/idle scanning



Statistisches

- Bei vielen ISP ist die Zunahme der DDOS spürbar (>10%) im Vergleich zum 1.Halbjahr 2002
- Meiste Attacken kleiner 50 Mbit/s
- Einzelne Attacken um Faktor 10 höher.
- Zunahme der non-spoofed DDOS Attacken mit Hilfe von „zombies“; privaten Rechnern hinter DSL
-

Lösung: CenterTrack

- Bei Uunet eingesetzt[2].
- Ziel ist die Erstellung eines Overlay-Netzes aus IP/MPLS-Tunnel, welches transparent auf eine Verbindung geschaltet werden kann.
- Kombination aus BlackHole-BGP, netflow-stats und Logauswertung
- Realtime-Monitoring; wird von Uunet aktiv eingesetzt.

Lösung: BlackHole-BGP

- Bei diversen Providern in Betrieb [3]
- Ist eine vereinfachte Variante des CenterTrack, wobei in einer zebra-Instanz Hostrouten an alle Router exportiert werden.
- Diese Routen zeigen auf JEDEM Backbone-Router des ISP auf ein reject-Interface und verwerfen den Traffic entsprechend.

War Story: Blackhole-BGP

- Eine Attacke findet statt ...
- Support bzw. NOC setzt per CLI oder GUI auf einem Routeserver (BGP) eine Route mit Tag
- Route wird exportiert und blockt Traffic zum Opfer.
- Logging auf das Tag bringt die Inbound-Interfaces hervor, von denen die DDOS originiert.

Ansätze der ISPs

- Zusammenfassung von diversen Methoden [4]:
- Pushback
- IP Traceback
- CenterTrack
-

Lösung: Pushback

- Mechanismus des rate-limit mit Signalierung an die Upstream-Router um NUR den DDOS-Traffic zu filtern, und legitimen Traffic durchzulassen.
- Simulierung im ipfw von FreeBSD erfolgreich, Umsetzung in IOS / Junos noch fraglich
- Weiteres Proposal von S. Bellovin[5]

War Story: Pushback

- Es wurde im AT&T Lab ein Router-Netz aufgebaut.
- Entsprechend dem Draft von Bellovin wurden ipfw Regeln definiert, die bei entsprechender Signalisierung greifen.
- Tests haben funktioniert, es mangelt aber an Umsetzung im Real Life.

Lösung: IP Traceback

- Erweiterung des Protocol-Stacks (IETF WG) lt. Vorschlag von S.Bellovin [6] um Informationen im IP-Header unterzubringen, welchen Weg das Paket genommen hat.
- Ziel ist die Zurückverfolgung von Attacken (->Quellrechner)
- Insofern nur sinnvoll bei gespooften Quelladressen, viele Attacken sind aber non-spoofed

Lösung: Fix your net!

- Initiative „smurf-amplifiers“ war ein Erfolg. Viele Netze wurden gefixt.
- Problem sind nicht mehr Netze, sondern private Rechner hinter Broadband-Netzen (xDSL/Cable)
- Awareness der DSL-Router-hersteller intensivieren -> Filter im DSL Router
- Aktuelle Patches einsetzen

Realitätsbezug

- Vorher benannte Möglichkeiten sind nur in gewissen Kontexten nutzbar, jedoch nicht als Gesamtlösung zu betrachten.
- Es ist die Community gefragt, eventuelle Ideen zu sammeln um eine gemeinsame Lösung zu finden.
- Einige Ideen folgen:

Idee 1: distributed block

- Koordination einer Instanz an zentralen Exchange-Points zwischen ISPs
- Announcen von Black-Hole Routen analog zu [3]
- „Trigger“-Möglichkeiten fehlen
- Idee wäre snort o.ä. zu modifizieren, um es in diesem Kontext nutzbar zu machen.

Idee 2: distributed pushback

- Nutzen einer distributed Infrastruktur um entsprechende Rechner zu blocken, bzw. um Filterregeln zu setzen.
- Alternativ: „Gegenattacke“ gegen Quelle
- NICHT zu empfehlen, aber dennoch sollte man es diskutieren

Idee 3: friendly virus

- Kombination aus Idee 1 (distributed block) um IP-Adressen zu sammeln.
- Distributed-friendly-Virus Attacke zu den Zombies um diese zu fixen (z.B. Originalfiles wieder einspielen)
- (Theoretisch) eine Möglichkeit

Zusammenfassung

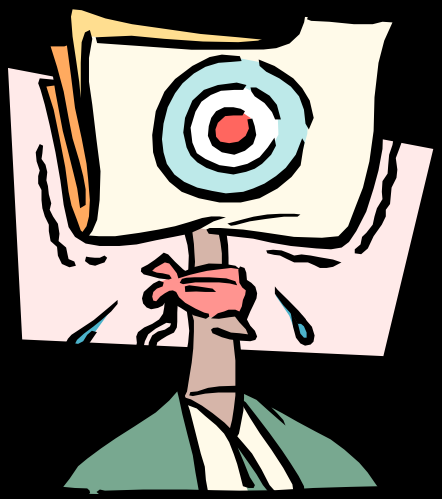
- Einige reaktive Methoden sind in Benutzung.
- Ziel ist eine proaktive Methode, um die DDOS-Angriffe einzudämmen bzw. sinnlos zu machen
- Friendly Virus scheint eine gewagte Methode zu sein, jedoch könnte vom Erfolg gekrönt sein.
- Aufklärungsarbeit für Enduser hilft nur bedingt.
-

Fragen ?

- Bevor wir zum 2. Teil (Workshop) übergehen, bestehen Fragen von Seiten des Publikums?
-

Workshop (2.Teil)

- Was wünscht sich der Nutzer ?
- Welche Methoden gibt es noch ?
- Welche Ideen gibt es noch ?

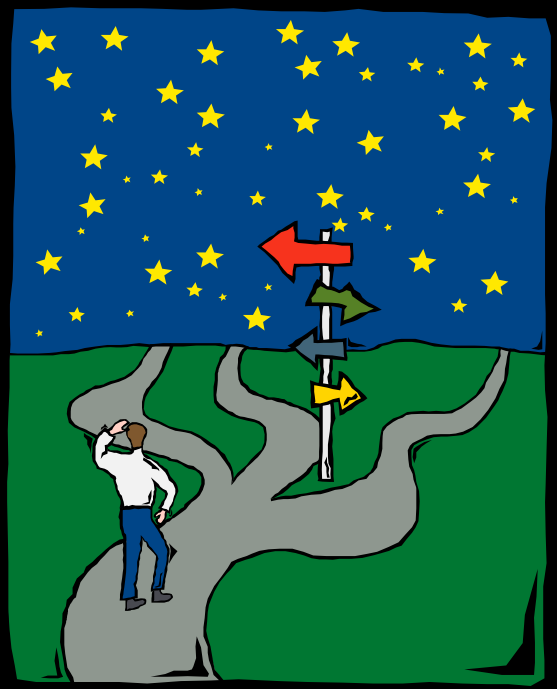


Denkansätze

- An welchen Netzpunkten ist es topologisch sinnvoll, Filter bzw. Regeln zu setzen?
-
  - Internet Exchanges
  - Zentral beim Provider (ISP/ Carrier)
-

Danke

-
- Vielen Dank für die Aufmerksamkeit



Resources/Links:

- [1] http://www.ripe.net/ripe/meetings/index.html
- [2] http://www.nanog.org/mtg-9910/robert.html
- [3] http://www.secsup.org/Tracking/
- [4] http://www.cymru.com/Documents/tracking-spoofed.html
- [5] http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/ioanni.pdf
- [6] http://www.research.att.com/~smb/papers/draft-bellovin-itrace-00.txt
-
- Vortrag ist zu finden unter:
-
- http://www.lambda-solutions.de/ddos/