IPv6-Darknet

Sven Schindler

Potsdam University / Beuth Hochschule Berlin

Berlin, June 12, 2013

Outline

Why do we need IPv6 dark- and honeynets

- huge IPv6 address space makes brute-force network scanning impossible
- research new scanning approaches
- how to analyse IPv6 related attacks
- weaknesses aimed at IPv6 design (THC)

This is not the first IPv6 darknet

- /48 experiment from 2006 reported 12 ICMPv6 packets within 16 months [1]
- IPv4 class A darknet in 2004 captured 30,000 packets/second [2]
- 9 days /12 IPv6 darknet experiment received 21,000 non-malicious packets (2010)
- we started our /48 darknet experiment in March 2012
- /48 Hurricane Electric SIT tunnel

Packet capturing

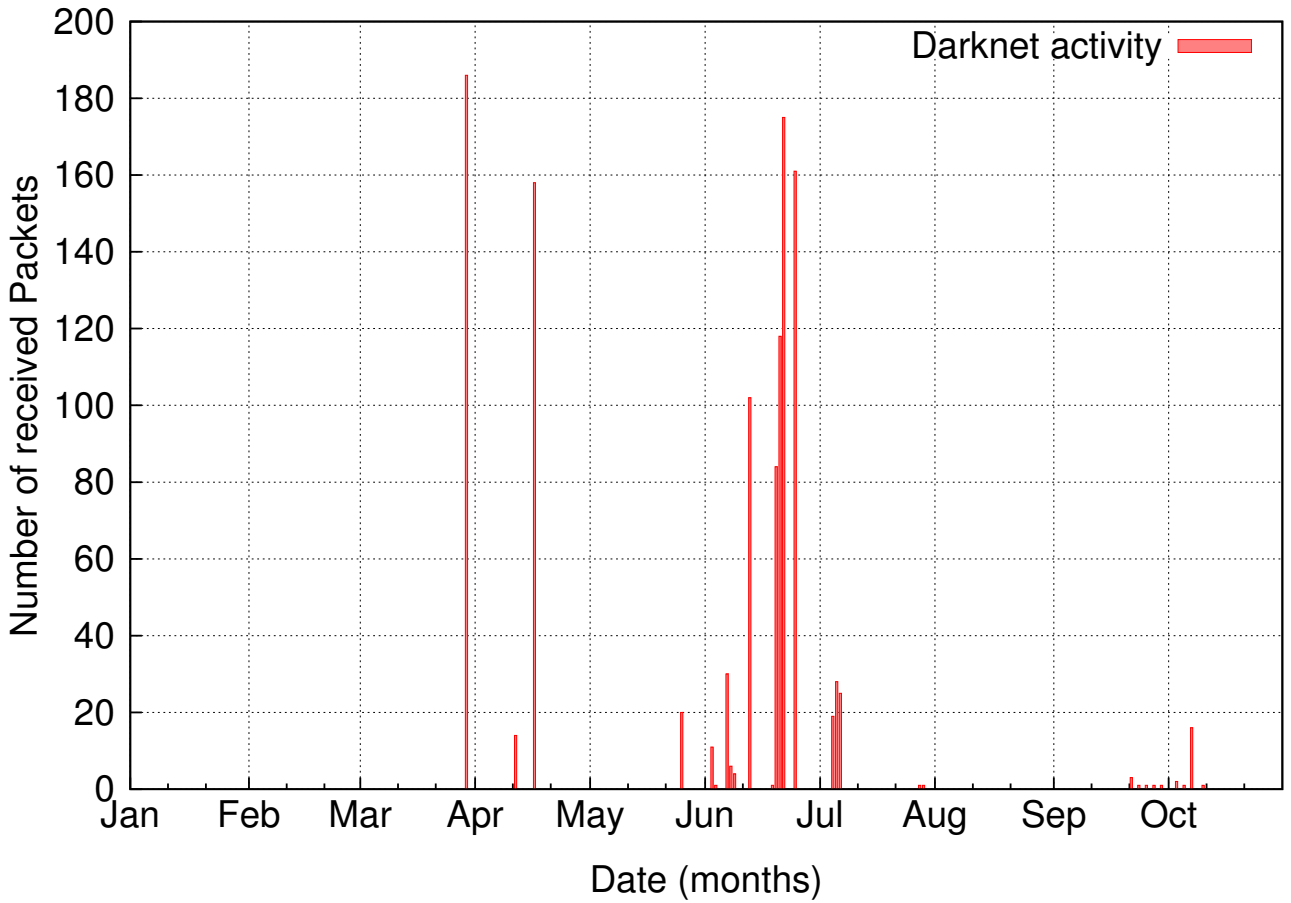
Capture Script

```
#!/bin/bash
IFACE=${1}
ROTATE=3600
CAPTUREDIR=/var/capture
FILEPREFIX=ipv6darknet-${IFACE}-

tcpdump -i ${IFACE} -G ${ROTATE}
  -w ${CAPTUREDIR}/${FILEPREFIX}'%s-%F-%H_%M_%S'.
     cap -s 0 -K -l -n -U &
```

Darknet results after 9 months

- 1172 packets received
- TCP traffic only
- most packets around IPv6 World Launch Day



Backscatter traffic

- 1157 packets seem to be backscatter
- caused by misconfiguration or spoofed source addresses

Number of packets	Source port	Description
486	113	auth
327	22	ssh
186	6667	ircd
158	80	http

Table: Source ports of the received backscatter packets.

Some interesting facts about the backscatter traffic

- port 113
  - belongs to Ident protocol (RFC1413)
  - 486 packets from 8 different sources to 457 different destinations
  - most packets contained the same acknowledgement number
- port 22
  - 327 packets from 8 different sources targeting 295 destinations
  - again: most packets contained the same acknowledgement number
- port 6667
  - 186 packets from the same source to different destinations
  - again: all packets contained the same acknowledgement number
- port 80
  - 158 packets from the same source to different destinations
  - all packets but one with the same acknowledgement number and target port

Ack Scans

- 15 packets with ACK flag only received
- from the same /64 subnet
- address space also from Hurricane Electric
- source port is 445

Summary

- traffic indicates spoofed source addresses
- DoS-attacks observed?
- threat level in IPv6 network still low compared to IPv4
- attackers interest in IPv6 networks is raising
- no connection attempts

References

Matthew Ford, Jonathan Stevens, and John Ronan.
Initial Results from an IPv6 Darknet.
In *ICISP '06: Proceedings of the International Conference on Internet Surveillance and Protection*, page 13, Washington, DC, USA, 2006. IEEE Computer Society.

Ruoming Pang, Vinod Yegneswaran, Paul Barford, Vern Paxson, and Larry Peterson.
Characteristics of internet background radiation.
In *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, IMC '04, pages 27–40, New York, NY, USA, 2004. ACM.