Pertahanan Ilmu Hitam

Budiwijaya / @budiwijaya

Siapa saya ?

Network Administrator - Wowrack

Koordinator Tim Infrastruktur - OI

Network Administrator - IIX-JI

Mau tau lebih? Try googling me.

Agenda

Serangan di Jaringan

Deteksi dan Pencegahan

Tanya Jawab

Network Engineer?

System Engineer/Administrator?

Security Engineer?

Programmer?

Serangan di Jaringan

P0D - Ping of Death

DoS - Denial of Service

DDoS - Distributed Denial of Service

dan banyak lagi..

Deteksi dan pencegahan

PPS(packet per second) tiap titik

Bandwidth Spike

Trends (cacti)

Treshold (zabbix/nagios)

Netflow/sFlow devices

NetFlow/sFlow collector

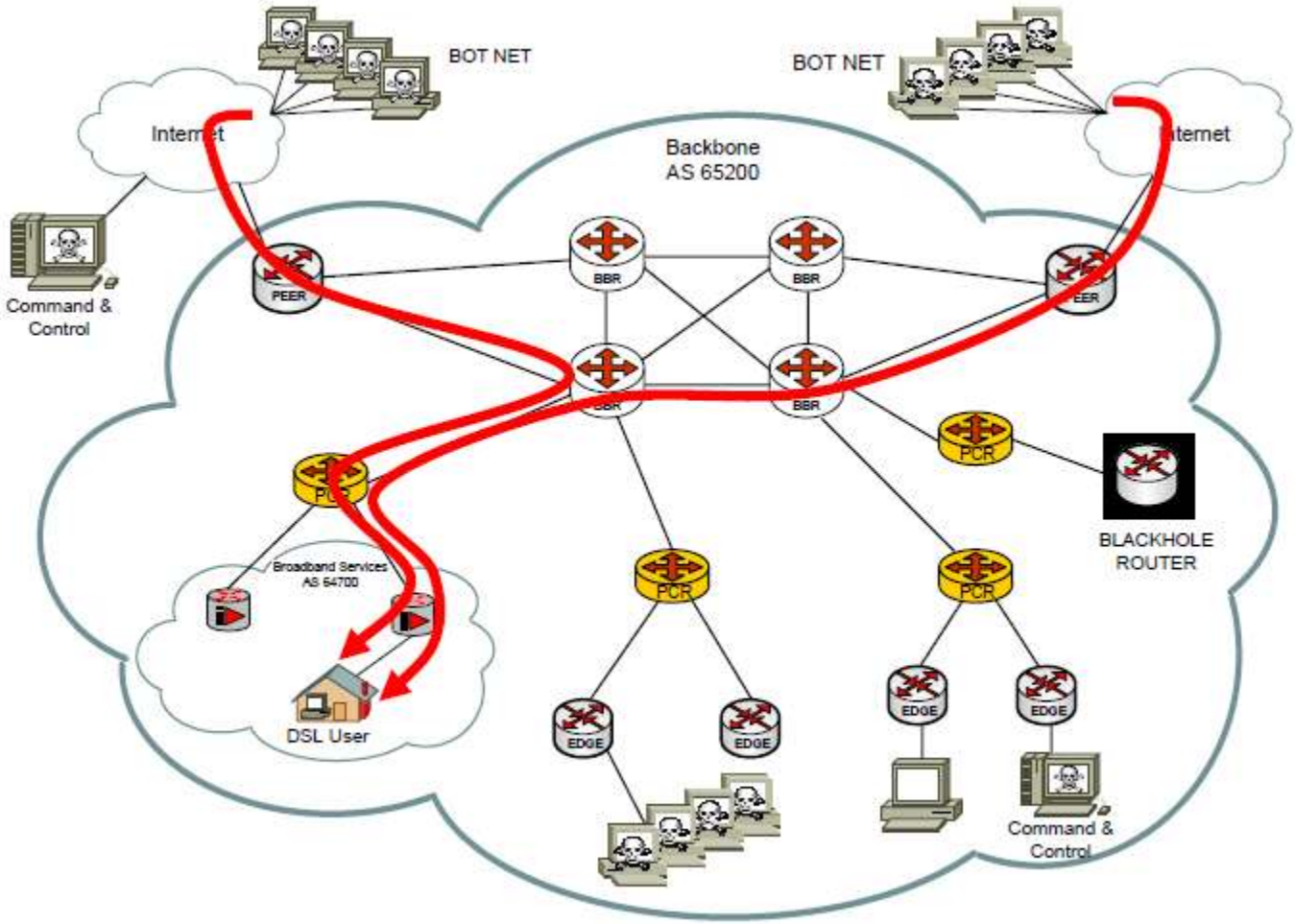
Deteksi dan pencegahan

Blackhole Routing

Sinkhole

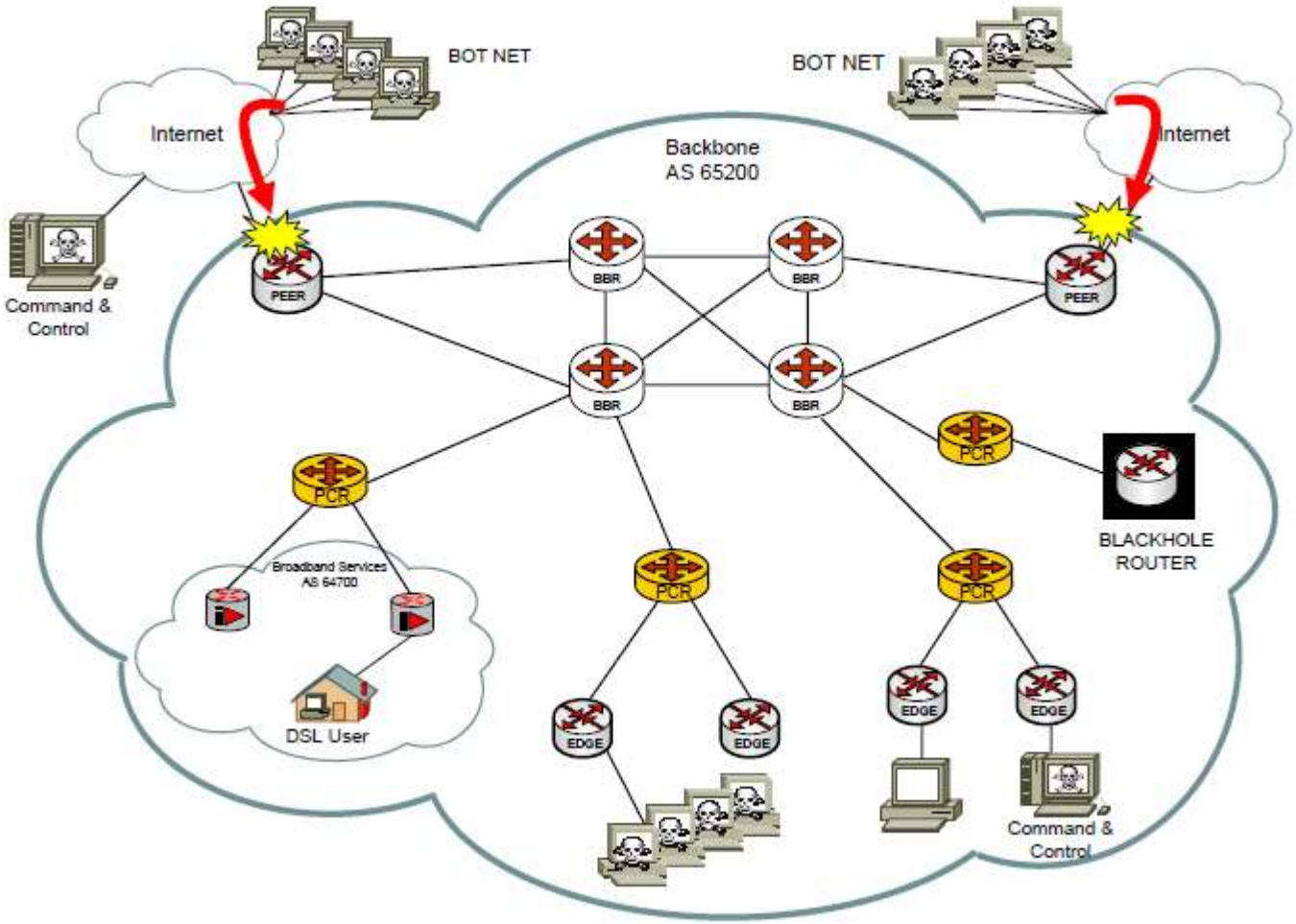
(honeypot of network infrastructur)

DDOS ke pelanggan



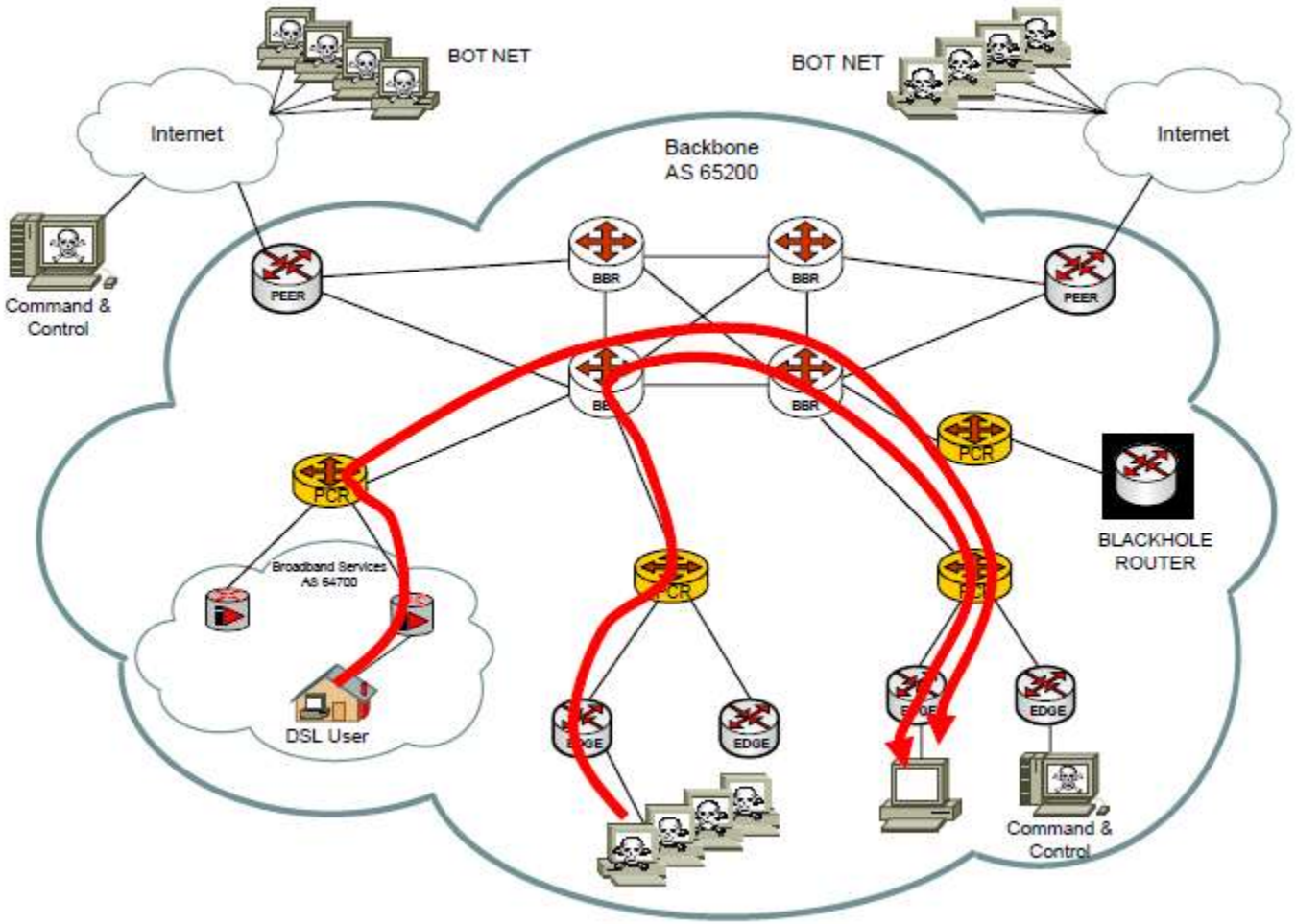
*1

DDOS ke pelanggan



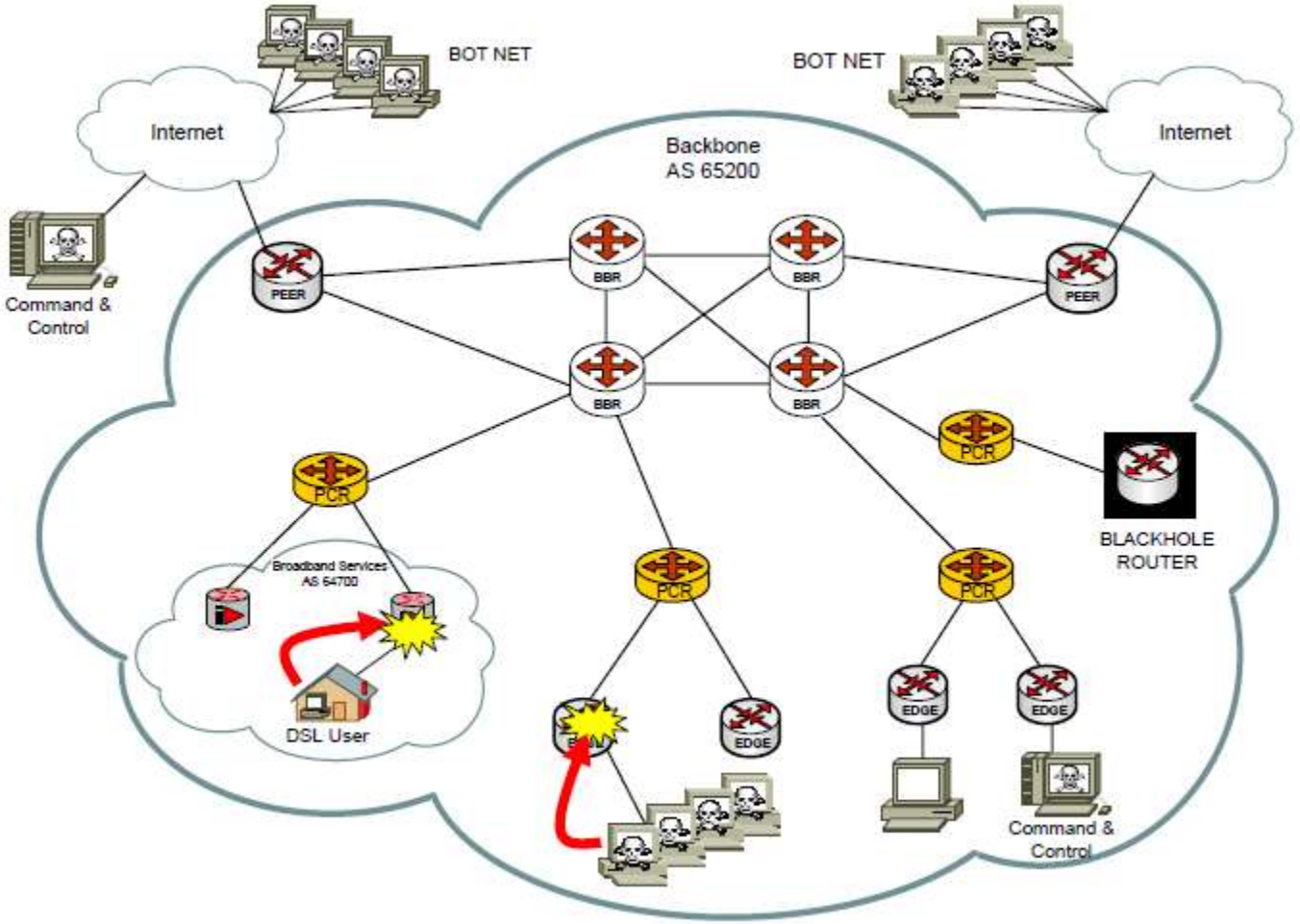
*1

DDOS dari pelanggan



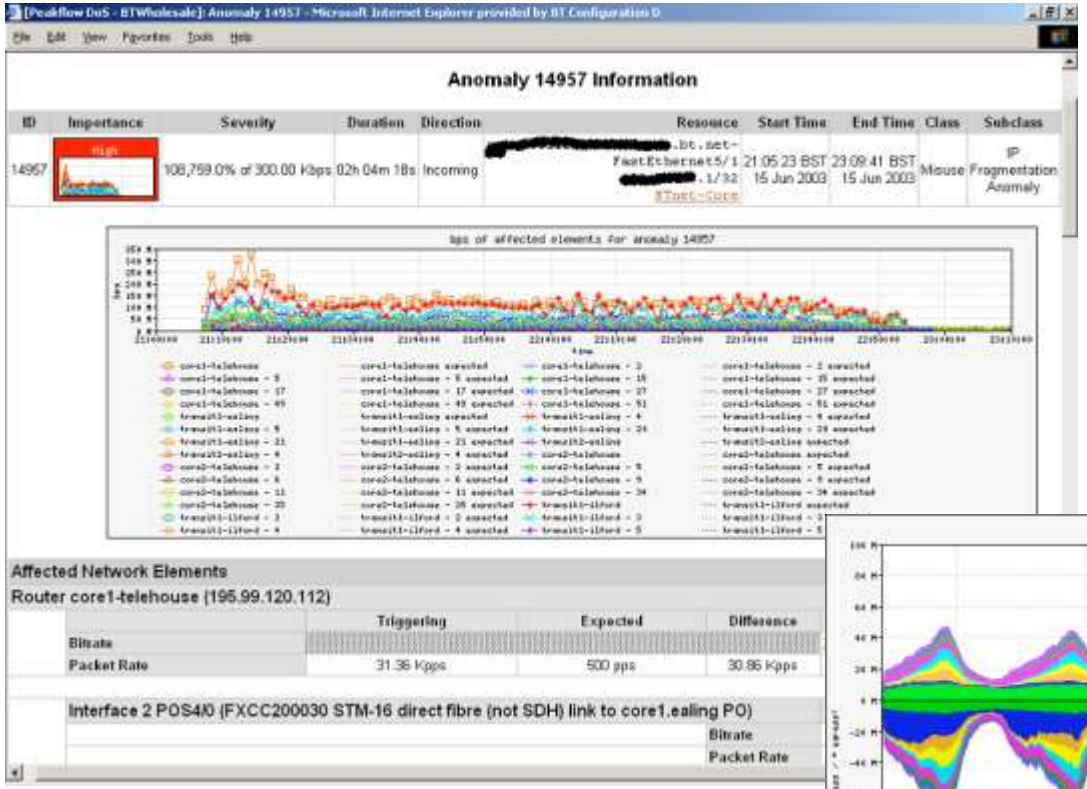
*1

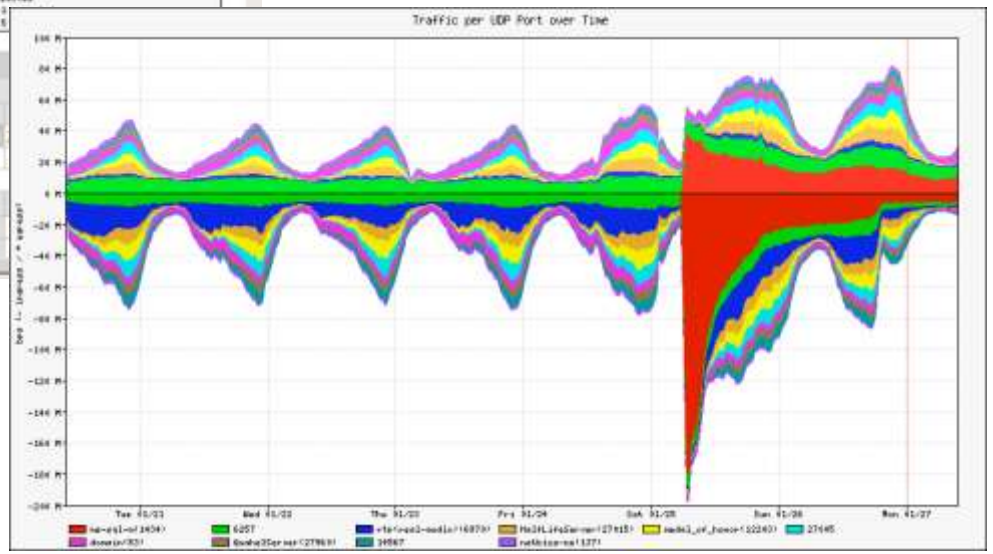
DDOS dari pelanggan



*1

Deteksi dan pencegahan





ntop – ntop.org
sflow collector – sflow.org

Peakflow – Arbor network

*2

Tanya Jawab

Terima kasih

081-55-000-332
e: bbuuddiiww@gmail.com
t: @Budiwijaya
(chat, share, proyek ?)

Sumber Gambar

1. http://www.nanog.org/meetings/nanog32/presentations/soricelli.pdf
2. http://www.nanog.org/meetings/nanog30/presentations/morrow.pdf