

Managing a DOS attack on Opentransit Network

Operational overview

Vincent Gillet, Jean-michel Valey

vgi@opentransit.net, jeanmichel.valey@francetelecom.com

This is an operational overview.

Read <http://www.nanog.org/mtg-0402/pdf/morrow.pdf> for blackhole technology.

- *24/7 “raw” Blackhole*
- *Automatic blackhole via BGP communities*
- *Blackhole v2 tool with extended feature.*
- *Customer web interface for effective blackhole*
- *Additional feature requested in v3.*

Raw blackhole via NOC

Free service rather successful :

In 2003, 88 requests to blackhole from 30 customers. 2004 : +/- 4 requests a week.

Intensively used by 4 or 5 customers (other 80% of the request comes from them)

Mostly used by low-capacity customers (E1 → oc12)

2 Blackhole types for different usage :

- Core

- ▶ *monitor running attack in blackhole itself. Only one chart to monitor*
- ▶ *Can implement a filter list to have real-time counters*
- ▶ *Security engineer can dump packets to get additional data.*
- ▶ *It does not scale : Core blackhole is only connected via many oc3s to backbone
→ may overload circuit.*
- ▶ *We have to carry bad traffic up to analyzer box*

- Edge

- ▶ *Thanks to null0 counters and discard interfaces , we have some hints on peer sending bad traffic in case of spoofed or non-valid ip address*
- ▶ *Good ; We do not carry bad traffic*
- ▶ *It scales well since Traffic is discarded at the edge.*

*→ NOC used to switch between core/edge blackhole depending on attacks.
Both provide good and different data.*


Raw blackhole via N O C

Blackhole on Opentransit - Microsoft Internet Explorer

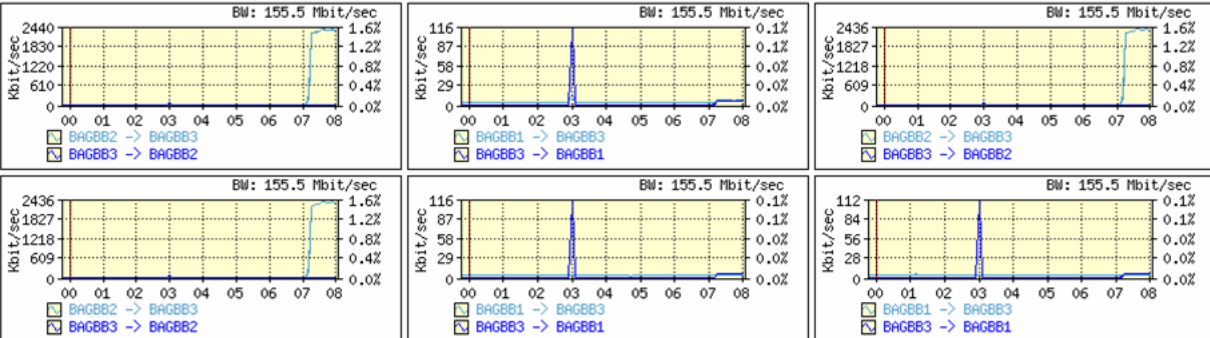
Fichier Edition Affichage Favoris Outils ?

Adresse <https://www.opentransit.com/cgi-bin/blackhole.pl>

Google

 /32 BlackHole on Opentransit

Traffic on BAGBB3 uplinks :



Existing **Manual** Blackhole on Mon Apr 5 08:03:14 2004

	IP	Date	Username	Ticket	Edge	BAGBB3 Count
<input checked="" type="checkbox"/>	61.3.165.2/32	Mon Mar 15 03:22:13 2004	igor	0403444240	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	168.234.201.194/32	Sun Mar 28 20:28:40 2004	jachaume	0403517494	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	168.234.201.195/32	Sun Mar 28 20:45:04 2004	jachaume	0403517494	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	200.157.215.20/32	Mon Apr 5 07:11:32 2004	Hume	0404552160	<input type="checkbox"/>	

Note 1 : Uncheck the Combobox and click Update to "un-blackhole" an IP address.
 Note 2 : Uncheck the "Edge" column to switch between Core and Edge blackholing.

Analysis done in the core

This is done only on demand for “valuable customers”

Sampling of packets and analyse on Blackhole box itself (use of tcpdump on Juniper)

monitor start /var/tmp/attack | match <Victim IP>

Apr 5 13:38:23 192.35.215.1 194.76.132.141 38941 22063 6 0x0 40 7 0x0 0x2

Apr 5 13:38:23 192.35.215.1 194.199.162.18 19724 31174 6 0x0 40 7 0x0 0x2

Apr 5 13:38:23 192.35.215.1 194.249.36.2 26803 64017 6 0x0 40 11 0x0 0x2

Apr 5 13:38:23 192.35.215.1 194.20.49.123 16507 29836 6 0x0 40 11 0x0 0x2

Apr 5 13:38:23 192.35.215.1 194.153.234.212 35939 50969 6 0x0 40 11 0x0 0x2

Use dedicated netflow export and collector to have immediate snapshot of attack type if not obvious (DOS vs DDOS, faked source, random ports, ...).

Tool provide Top 10 flows for many criteria ...[netflow_analyse.html](#)

.... and mail to Top offender [DDOS_notif.txt](#)

Look for null0 counter increase during edge/core blackhole change.

→ One router is obviously impacted → Attack comes from 1 peer (we have some well known “bad guys”)

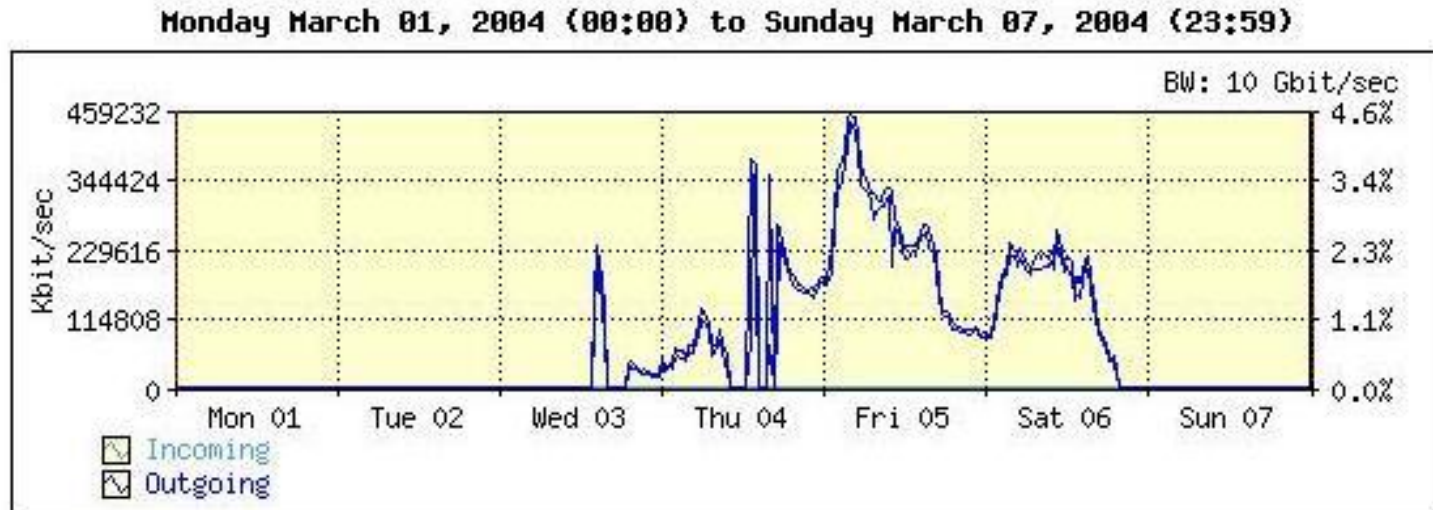
→ NOC Implement an ACL on suspected peer if we can (Engine issues). If acl is not possible : Blackhole on this box only thanks to local static route.

→ Many routers show increase → this is mostly a DDOS

If attack comes mostly from an area, blackhole this area only thanks to new blackhole tool v2 (to come)

Analysis done at the edge

NULL0 Graph



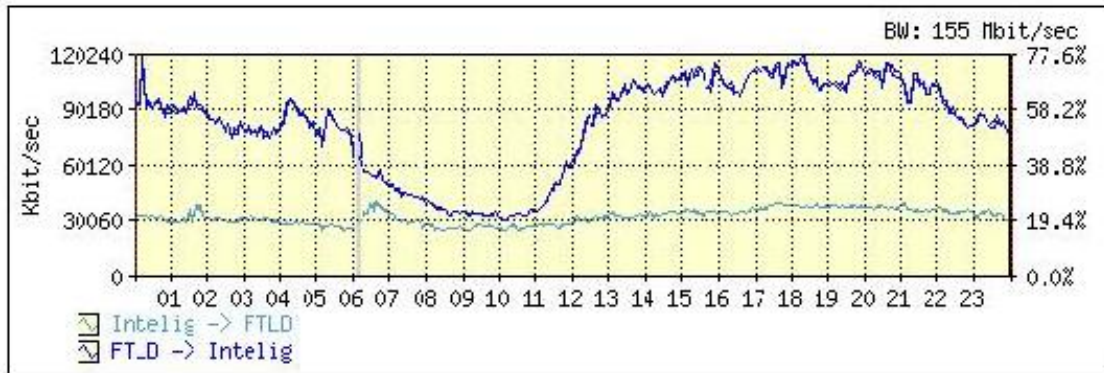
NULL0 tool for live monitoring :

null0 interface counter (~30 sec) in bit/sec : 16:15:45

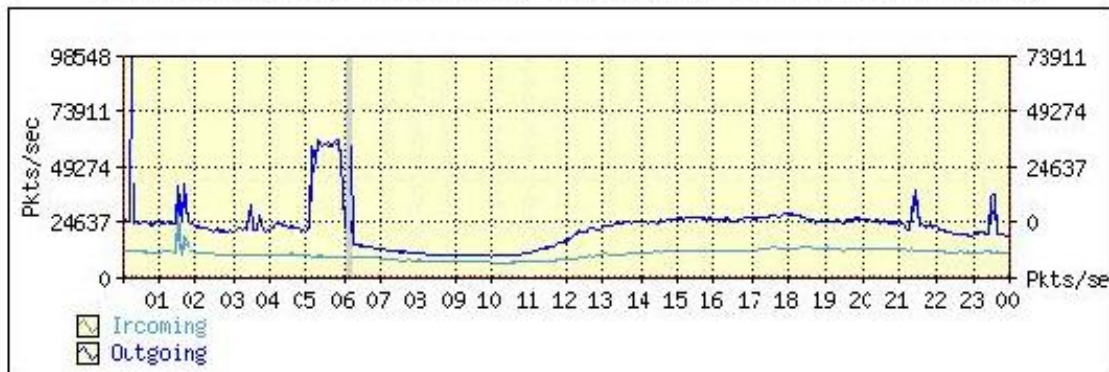
	Actual	Change
PARIS1	16.2 M	4.2 M
PALOALTO2	12.0 M	-53.4 K
TOKYO1	5.0 M	-569.8 K
MADRID2	4.2 M	154.3 K
LONDON3	435.9 K	-19.9 K
HONKHONG2	421.3 K	-318.0 K

Analysis done at the edge

Compare *bits* and *packets* counters. Snapshot :



Wednesday March 24, 2004 (00:00) to Wednesday March 24, 2004 (23:59)



Analysis conclusion

Very time consuming thus this is not done for every attacks.

Attacks are rather similar thus analysis would be useful for next attacks.

*Analysis need high skilled engineer thus cannot be done on 24/7 based.
This is best effort.*

If analysis is not possible, customer has “at least” blackhole feature that can save money (traffic is not billed) and connectivity.

Noc check every 24 hours that attack is still running and notify customer if blackhole can be removed. Customers used to “forget” blackholed /32.

Proposed to customers as a paid option :

- *Customers are excited by “do it yourself” feature, but does not understand complexity :*
 - *our Security team have to help them to implement.*
May look easy for skilled BGP engineer, but not for raw customers ☺
 - *Since we provide same feature via 24/7 noc, they prefer “manual” way.*
- *Prevent blackholing mistake from customer,*
 - ➔ *Make and maintain a prefix-list “blackhole candidate”.*
- *We cannot monitor attack our self.*
 - ➔ *Huge attack may overload our core blackhole.*
 - ➔ *Attacks may be over but customer keeps blackholing.*

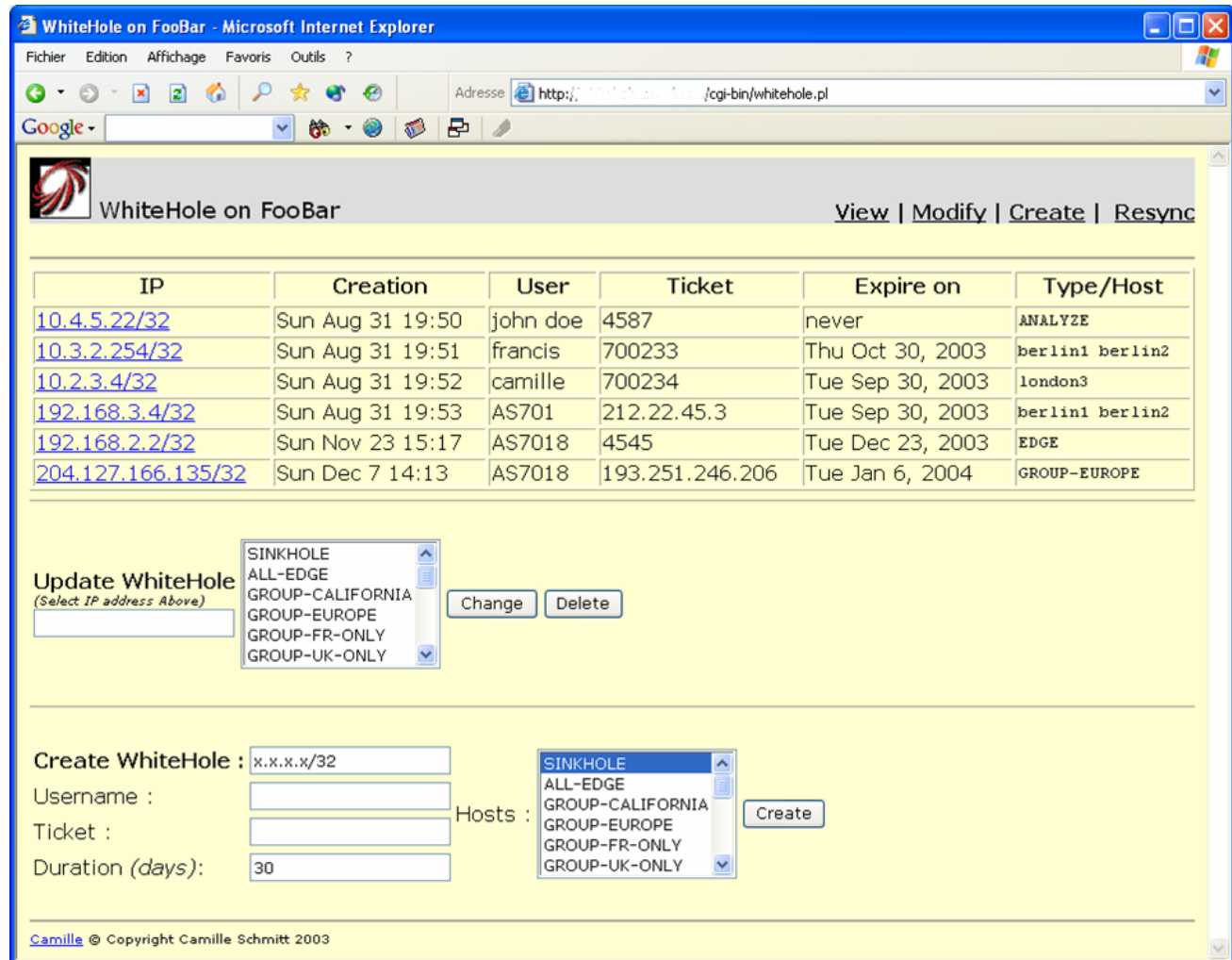
NOC need better blackhole tool :

- *Any blackhole change today make all blackholed ip flapped (poor implemenation done 18 months ago)*
- *Edge vs Core change is very useful to detect origin.
→ Should be smooth (no flap).*
- *Need to restrict edge backhole at some box or area
→ Regional blackhole to keep providing 80% connectivity to the customer*
- *Need for automatic monitoring and sampling*
 - *Dedicated graph for each blackholed ip*
 - *Sample of packet during 5 seconds and display.*
- *Need for automatic expiration mechanism*
 - *Blackhole should be removed automatically if not updated after n days.*

Blackhole v2 N O C interface

Snapshot :

(live demo)



WhiteHole on FooBar - Microsoft Internet Explorer

Adresse <http://.../cgi-bin/whitehole.pl>

WhiteHole on FooBar [View](#) | [Modify](#) | [Create](#) | [Resync](#)

IP	Creation	User	Ticket	Expire on	Type/Host
10.4.5.22/32	Sun Aug 31 19:50	john doe	4587	never	ANALYZE
10.3.2.254/32	Sun Aug 31 19:51	francis	700233	Thu Oct 30, 2003	berlin1 berlin2
10.2.3.4/32	Sun Aug 31 19:52	camille	700234	Tue Sep 30, 2003	london3
192.168.3.4/32	Sun Aug 31 19:53	AS701	212.22.45.3	Tue Sep 30, 2003	berlin1 berlin2
192.168.2.2/32	Sun Nov 23 15:17	AS7018	4545	Tue Dec 23, 2003	EDGE
204.127.166.135/32	Sun Dec 7 14:13	AS7018	193.251.246.206	Tue Jan 6, 2004	GROUP-EUROPE

Update WhiteHole
(Select IP address Above)

- SINKHOLE
- ALL-EDGE
- GROUP-CALIFORNIA
- GROUP-EUROPE
- GROUP-FR-ONLY
- GROUP-UK-ONLY

Create WhiteHole :

Username :
 Ticket :
 Duration (days):

Hosts :

- SINKHOLE
- ALL-EDGE
- GROUP-CALIFORNIA
- GROUP-EUROPE
- GROUP-FR-ONLY
- GROUP-UK-ONLY

Camille © Copyright Camille Schmitt 2003

Customers are much more familiar with Web than BGP ☺


- *Let customer blackhole it's _OWN_ IP address
Check that /32 requested belong to Customer*
- *Let customer to mitigate blackhole drawbacks
Give regional blackhole.*
- *Fast blackhole (60 seconds)*
- *Easy to monitor (blackhole/unblackhole and see immediate effect)*
- *Automatic expiration mechanism*
 - *Blackhole automatic expires after n days (7 days maximum).*
- *Noc get automatic notification for each new blackhole.*

WhiteHole on FooBar - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

Adresse <http://whitehole.zoreil.com/cgi-bin/protected/whitehole.pl>

Google

 WhiteHole on FooBar for AS7018 [View](#) | [Modify](#) | [Create](#)

IP	Creation	User	Ticket	Expire on	Type/Host
192.168.2.2/32	Sun Nov 23 15:17	AS7018	4545	Tue Dec 23, 2003	EDGE
204.127.166.135/32	Sun Dec 7 14:13	AS7018	193.251.246.206	Tue Jan 6, 2004	GROUP-EUROPE

Update WhiteHole
(Select IP address Above)

ALL-EDGE
GROUP-CALIFORNIA
GROUP-EUROPE
GROUP-FR-ONLY
GROUP-UK-ONLY
atlanta1

Create WhiteHole : Hosts :

ALL-EDGE
GROUP-CALIFORNIA
GROUP-EUROPE
GROUP-FR-ONLY
GROUP-UK-ONLY
atlanta1


Terminé

WhiteHole on FooBar - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

Adresse <http://whitehole.zoreil.com/cgi-bin/protected/whitehole.pl>

Google

 WhiteHole on FooBar for AS7018 [View](#) | [Modify](#) | [Create](#)

ERROR :

This IP address does not belong to you (AS7018) but AS3215.... Request denied.

[Camille](#) © Copyright Camille Schmitt 2003

Terminé

Internet

- *Blackhole for not-BGP customers*
- *Provide a monthly report about blackhole activity.*
- *Provide real-time statistic for each blackhole*
→ *Remove blackhole (and notify) if attack is over.*
- *Provide ascii dump and analysis of sampled traffic.*
- *Monitor Customer Interface and raise an Email warning for odd Mbit/s vs pkt/s ratio. (see slide 8)*

Questions ??



Thank you