INTERNET PROTOCOL (IP) BLACK HOLES

Authors:

C.S. Krishnadev
Institute of Technology &Management
Gwalior-4754001 (MP)
E-mail: krishna_dev@yahoo.com

Prashant,
4th Year student,
IIITM (Deemed University),
Gwalior- 474003 (MP).
E-mail: prashant_iiitmg@yahoo.com
Phone No: 0751-2450982/2449601

Abstract

The concept of Internet Protocol (IP) Black Holes is a very exciting area of Network Security and Hacking. IP Black Holes is an active area of research and as the word suggests IP Black Holes do really exist on the Internet. These Black Holes are a very active phenomenon which can be a potentially lethal weapon in the armory of hackers and crackers alike. IP Black Holes are those unprecedented dangerous regions which get developed on the internet which act as potential black holes for packets going in those directions and get lost in the IP black hole world. Internet Protocol Black hole is defined as that area of the IP space for that there is no relevant routing information, right in the point where that information should have existed. In other words a certain entity is considered to be the destination for that zone, but the entity itself does not know how to route that zone. Black holes occur in the routing protocols especially in BGP (Border Gateway Protocol) context. Possible causes of black holes are an intended attack, a miss-configuration or an administrative action. Hence this paper is an attempt in the direction of highlighting the fact that IP Black Holes can be a potentially lethal hacking tool in the hands of hackers and crackers and carry a lot of security threat with them. We are proposing here that IP Black Holes can be even created intentionally by hackers and computer geeks and can lead to a very powerful attack on the very backbone structure of the Internet itself. A new concept of IP White Holes, which are symmetrically opposite to IP Black Hole concept, is also introduced here.

Keywords: Internet Protocol, Black Holes, Sink Holes, BGP, RIS, DoS, BCP, CIDR.

" In natural science, Nature has given us a world and we're just to discover its laws. In Computers, we can stuff laws into it and create a world. "

-Alan Kay

1. Introduction

The field of information security is an everlasting field of turmoil and sweating. Digital attacks are being waged every moment. Defenses are being shattered, attacks and counter attacks are being planned every now and then thus Alan Kay has aptly said that in computers we can stuff laws and create a world. Creativity and innovation in the field of Computer and Information Security are but very common phenomenon, since the human brain can go to any length of wildness in this regard. The basic trait of human being is to think destructively and it takes its toll on the day to day security incidents on the Internet. In this ever changing world of bits how about taking some ideas from Physics and redefining the very definitions of security, this urge gives birth to the concept of Internet Protocol (IP) Black Holes, a potentially lethal phenomenon which can shake the fabric of the Internet itself. Imagine regions on the Internet that can only engulf network traffic or those innocent packets that happen to pass by. Some day these gravitating IP black holes may choke the digital pipelines of the world potentially sabotaging the Internet traffic at its very grass root levels. These IP Black Holes like those in the interstellar Space can even increase in size and create an enormous sucking power to engulf the packets moving on the Internet. To our dismay they are not an inherent phenomenon of the internet created by its dynamics but can be implanted at critical internet junctures by hackers to sabotage the traffic of that region and in the long run the whole network traffic itself.

Internet Protocol is the basic protocol on which Internet runs governed by the IP address space allocation. Due to the very dynamics of the internet it creates a situation where the total IP address space allocated to a region is not reflected in the router logs of the core routers of that region. This phenomenon suggests that certain IP addresses are unreachable from the Internet though they are connected to the Internet, hence baby black hole forms in those regions. Internet Protocol Black hole is defined as that area of the IP space for, which there is no relevant routing information, right in the point where that information should have existed. In other words a certain entity is considered to be the destination for that zone, but the entity itself does not know how to route that zone. Hence packets which are destined for that region are lost in the routing fabric or are looped inside the black hole network and are destroyed when there TTL gets over. Thus black holes act as packet suckers created by the wrong routing table configuration on the entry routers to a particular network. Though security administrators can also deliberately create black holes so that the unwanted traffic can be dumped and not allowed to flow on the network creating unnecessary congestion. But black holes can also be created at critical points by hackers by compromising core routers and dumping useful traffic. Thus black holes are also synonymous to sink holes.

2. IP Black Holes: A Hackers perspective

In this section we will give some statistics of the creation of Black Holes in the Autonomous Systems and then we will discuss the protocol mechanism which leads to black hole creation and at last how they can be lethal in the hands of hackers. The following figure shows the number of black hole IP addresses in the given range of IP address allocations. This data has been compiled from the router logs of APNIC Autonomous System.

We can clearly infer that black hole activity is more pronounced in the IP range of 76.204.0.0 which is a Class B network hence a very large network is under black hole activity.

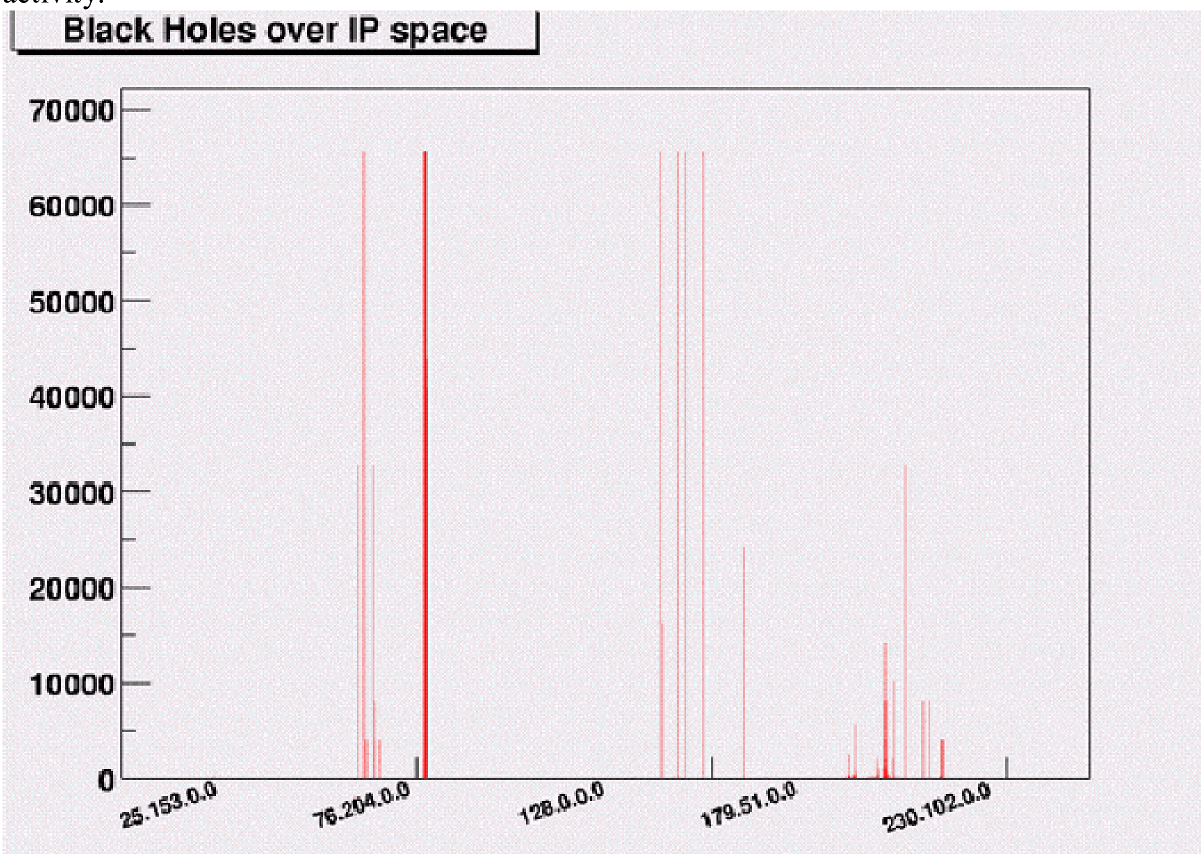


Figure 3. Black holes example – 17/04/2002 00:00

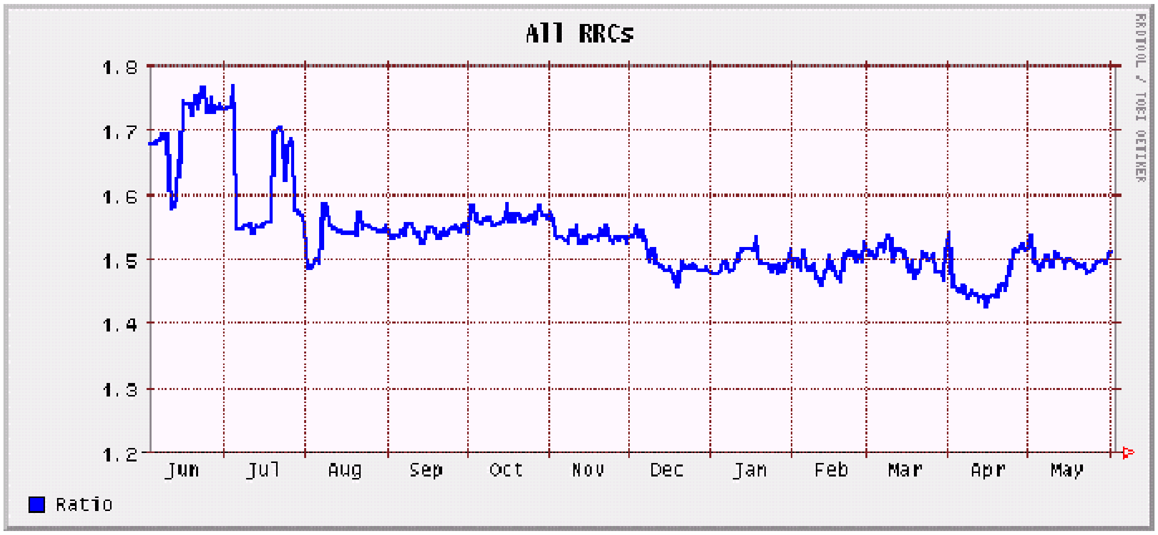


Figure 4. Prefixes after aggregation versus Prefixes after species removal

The blue wiggle line in figure above shows a clear decreasing overall trend. This ratio shows the efficiency of aggregation by the ASs as a cumulative figure. If this ratio tends to 1 or is decreasing means that the ASs in whole is more efficient in aggregating IP space. As we have a decreasing trend line, it means that ASs are really good in reorganizing there managed address space so that more aggregation is done there. This is a positive thing.

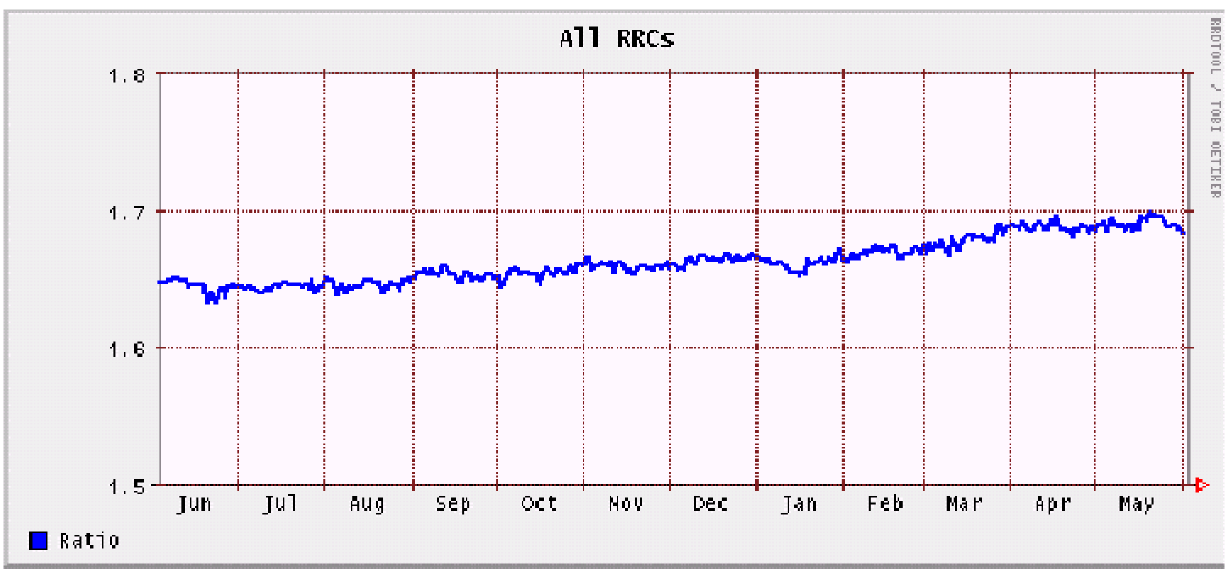


Figure 5. Prefixes after specifics removal versus Prefixes after specifics removal and aggregation

This ratio in the above figure gives us information about the efficiency of space allocation made to the ASs by the Regional Registries. The graph refers only to the space announced. If this ratio tends to be low, it means that the allocated and announced IP space is contiguous and fully announced. In our case we can see a small increase. This is fairly good behavior, knowing that registries try to keep up with ever growing demand for IP space. It means that they are keeping up, and more, they are doing a good job, since the increase trend is constant and not having huge hops.

2.1 Protocol Overview

The protocol mechanism that leads to black hole creation is given as follows. Before a host can send IP datagrams beyond its directly attached subnet, it must discover the address of at least one operational router on that subnet. Typically, this is accomplished by reading a list of one or more router addresses from a (possibly remote) configuration file at startup time. On multicast links, some hosts also discover router addresses by listening to routing protocol traffic. Both of these methods have serious drawbacks: configuration files must be maintained manually -- a significant administrative burden -- and are unable to track dynamic changes in router availability. Eavesdropping on routing traffic requires that hosts recognize the particular routing protocols in use, which vary from subnet to subnet and which are subject to change at any time. Here we specify an alternative router discovery method using a pair of ICMP messages, for use on multicast links. It eliminates the need for manual configuration of router addresses and is independent of any specific routing protocol.

The ICMP router discovery messages are called "Router Advertisements" and "Router Solicitations". Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if (and only if) no advertisements are forthcoming. The host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently starts up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements. (Increasing the rate of advertisements accommodates Links that suffer high packet loss rates or frequent partitioning, rather than increasing the number of solicitations that hosts are permitted to send.)

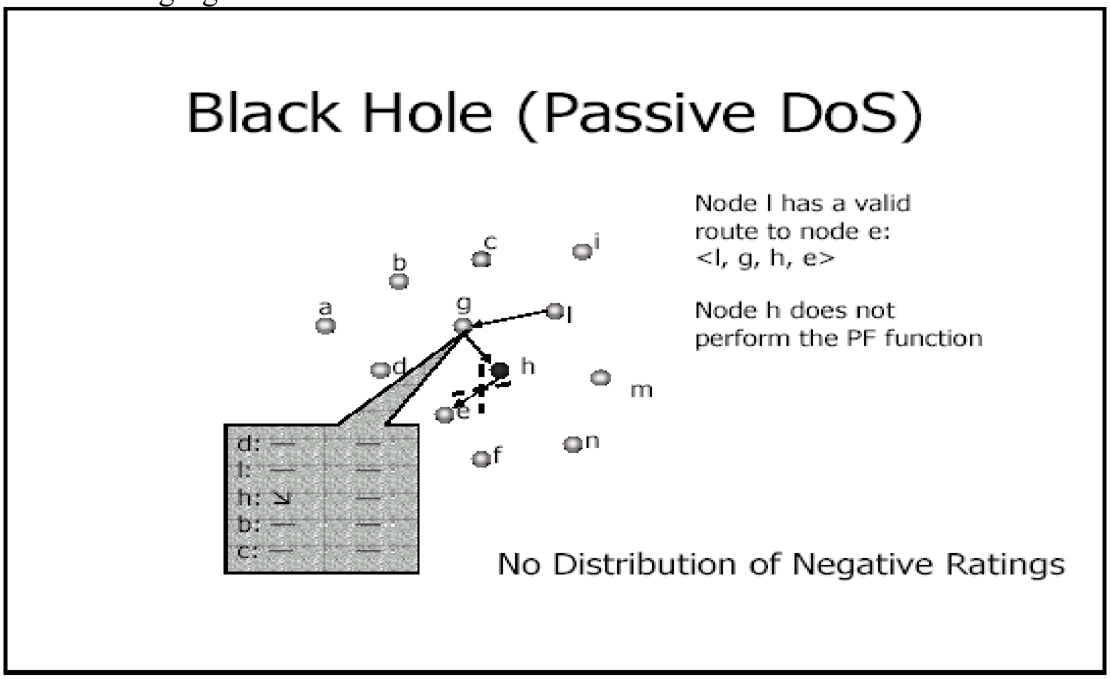
The router discovery messages do not constitute a routing protocol: they enable hosts to discover the existence of neighboring routers, but not which router is best to reach a particular destination. If a host chooses a poor first-hop router for a particular destination, it should receive an ICMP Redirect from that router, identifying a better one.

A Router Advertisement includes a "lifetime" field, specifying the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts, in the absence of further advertisements. This is used to ensure that hosts eventually forget about routers that fail, becomes unreachable, or stop acting as routers.

The default-advertising rate is once every 7 to 10 minutes, and the default lifetime is 30 minutes. **This means that, using the default values, the advertisements are not sufficient as a mechanism for "black hole" detection, i.e., detection of failure of the first hop of an active path -- ideally, black holes should be detected quickly enough to switch to another router before any transport connections or higher-layer**

sessions time out. It is assumed that hosts already have mechanisms for black hole detection, as required by hosts cannot depend on Router Advertisements for this purpose, since they may be unavailable or administratively disabled on any particular link or from any particular router. Therefore, the default advertising rate and lifetime values were chosen simply to make the load imposed on links and hosts by the periodic multicast advertisements negligible, even when there are many routers present. However, a network administrator who wishes to employ advertisements as a supplemental black hole detection mechanism is free to configure smaller values.

Also IP Black Holes can be used as passive Denial of Service attack method as given in the following figure:

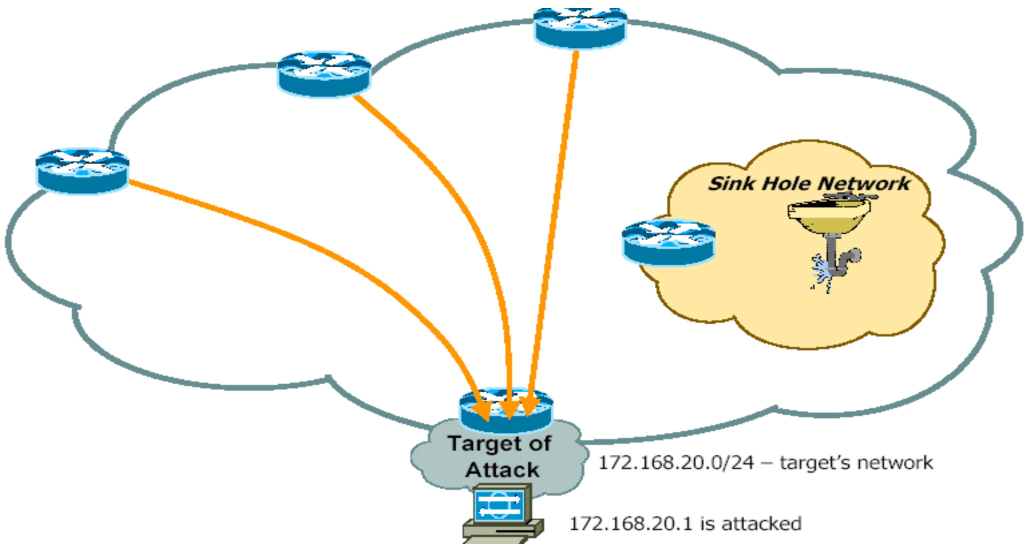


In this case a hacker can takeover the router 'h' so that if 'i' node wants to reach 'e' it cannot do since hacker has created a packet black hole at router 'h' which does not allow forwarding of IP packets to the destination router 'e'. This is a very simple example to demonstrate what black holes can do if deployed at security critical points on the Internet. Thus black holes can be created by hackers by compromising sensitive and mission critical routers and altering there routing tables to create a black hole region for sucking packets on the network. Black Hole technique is a passive DoS method rather than an active DoS method since here they disrupt the network traffic by providing only one way traffic for the packets but do not actively attack the hosts on the network. Thus passive way of black holing is an effective method to sabotage the IP traffic and also remain concealed from the security administrators eyes for some time.

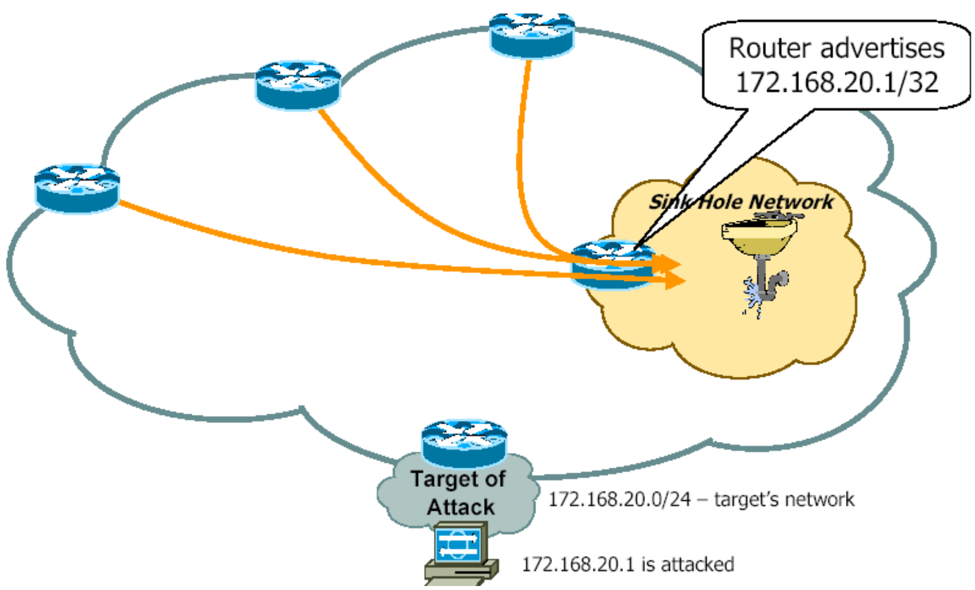
3. IP Black Holes: An Administrators perspective

In this section we will discuss black hole technique in the hands of an administrator. Black Holes or Sink Holes are the network equivalent of a honey pot. BGP speaking Router or Workstation that is built to *suck in* attacks. Used to redirect attacks away from the customer – redirect the attack on a router built to withstand the attack.

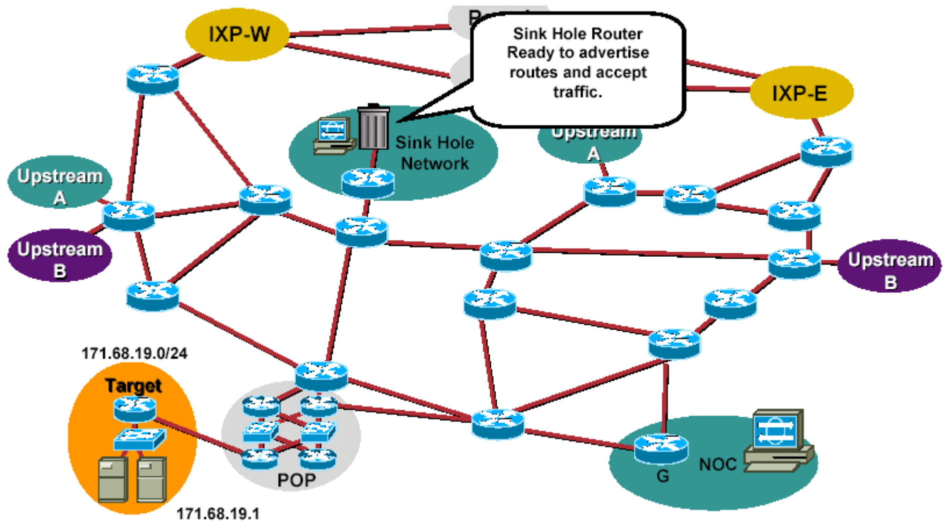
Used to monitor *attack noise, scans,* and other activity (via the advertisement of default router)



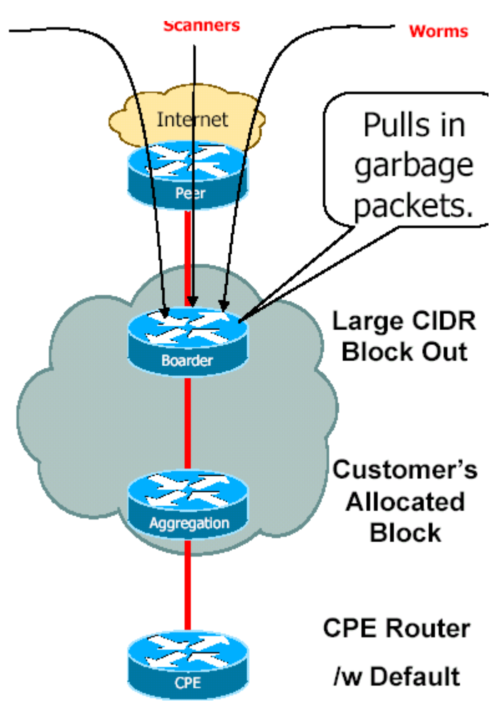
We know that ISPs who have for Attack Mitigation, Network Scans, Failed Attacks, Worm Infection Detection use the Black Hole technique to subvert an ongoing attack from the main target. Protecting the Backbone Point-to- Point Interface addresses. Managing DOS Flaps and customer traffic when circuits flap.



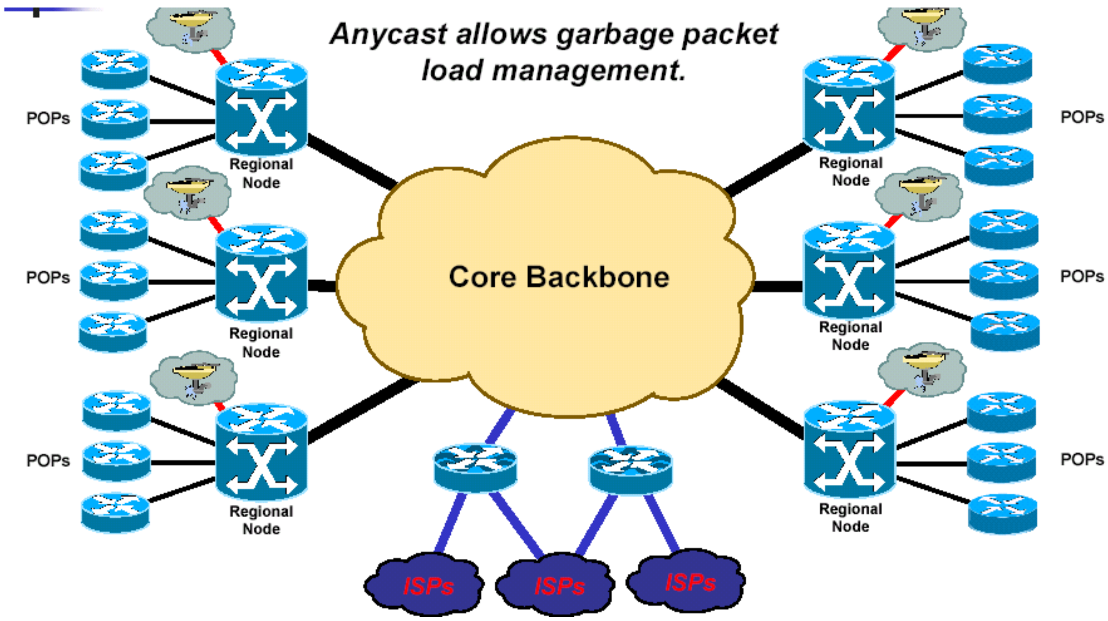
The mechanism by which Black holes or sinkholes are developed so that they can act as effective tool to counter an ongoing potential Denial of Service attack over the network is shown in the following figure in next page:



Sink Hole deployments are proving to be valuable ISP Security Tool. One of the reasons for this value is built on the premise that you sink undesirable packets to a planned location. This same characteristic is created with the BCP techniques used to advertise CIDR prefixes into the Internet. BCP is to advertise the whole-allocated CIDR block out to the Internet. Left over unallocated Dark IP space gets pulled into the advertising router. The advertising router becomes a Sink Hole for garbage packets.
A generic Sink/Black Hole architecture is shown below:



The figure above shows a generic IP Black Hole in which it sucks in the unwanted traffic in the form of network scans, worms, viruses, DoS attack packets etc. into the default router, which acts as an ultimate packet vacuum cleaner. Though routers are not actually designed for sucking in the network traffic or dumping the traffic but this functionality can be brought in to the routers by configuring them to drop packets coming over any interface into NULL0 interface in case of Cisco or Juniper routers. Thus artificial sinkhole regions can be developed by security administrators to drop unwanted traffic over them so that not only the hassle of moving back and forth the unwanted traffic is reduced but also major traffic congestion due to unwanted ACKs and NACKs are also avoided. The following network dig. shows a general deployment of IP Black Holes attached to regional nodes which are then connected to the core backbone network.

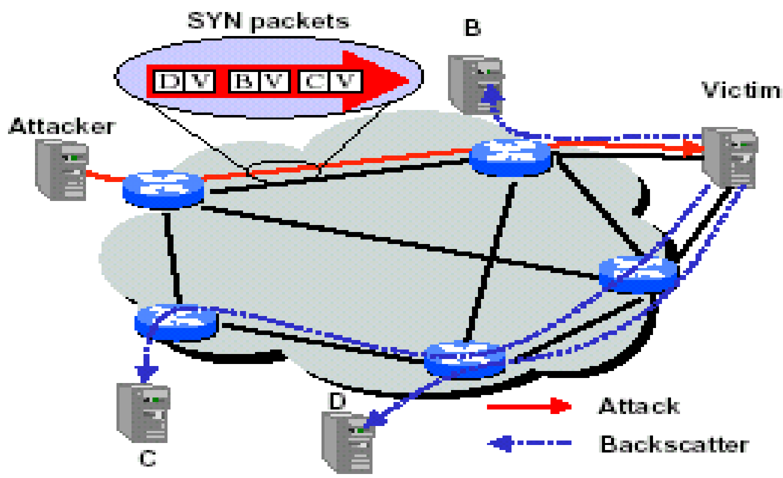


3.1 Backscatter Analysis: Estimating the Denial-of-Service activity on the Internet:

So how exactly do we decide that a particular host, Intranet or a WAN is under a DoS attack, so that we can engage an IP-Black Hole countermeasure. The most seminal paper presented with regard to quantifying the DoS attacks [1] needs to be referred. We will touch the technique of Backscatter analysis briefly here.

The attackers commonly spoof the source IP address field to conceal the location of the attacking host. Most programs select source addresses at random for each packet sent. (Something easily achieved by Dos Tools like TFN, Trinoo, Tribal flood etc.) When the spoofed packet arrives at the victim, the victim usually sends what it believes to be an appropriate response to the faked IP address. Occasionally an intermediate network device (such as router, load balancer, or firewall) may issue its own reply via an ICMP message. Again these ICMP messages are sent to the randomly spoofed source addresses.

Because the attacker's source address is selected at random, the victim's responses are equi-probably distributed across the entire Internet address space an inadvertent effect termed as **"Backscatter"**.



A generic Backscatter technique is shown in the figure above.

3.1.1 Quantification of Backscatter Analysis

Assuming per-packet random source addresses, reliable delivery and one response generated for every packet in an attack, the probability of expecting an attack is given by

$$E(X) = nm/2^{32}$$

Where the probe is monitoring "n" distinct IP addresses and any one host suffers an average attack of "m" packets. By observing a large enough address range it is possible to sample all denial-of-service activity on the Internet. Contained in these samples are the identity of the victim, information about the kind of attack, and a timestamp from which we can estimate attack duration. It is also possible to the average rate of unsolicited responses directed at the monitored address range to estimate the actual rate of the attack being directed at the victim, as follows

$$R \geq R' \ (2^{32} /n)$$

Where R' is the measured average inter-arrival rate of Backscatter from the victim and R is the extrapolated attack rate in packets-per-second. Hence Backscatter technique can be used to find an ongoing Dos attack and then take active countermeasures to configure or redirect the attacking packets to be dumped into the administratively made Black Hole or Sink Hole network region in the administrative domain of the ISP. Backscatter technique can act as the precursor to the triggering of the Sink Hole for taking an effective countermeasure in the form of a passive Black Hole deployment to dump the unwanted packets without creating further backscattering of the victims reply to the Internet.

4. **IP White Holes: A proposed new phenomenon**.

Hence as symmetry is the basic principle of Nature we here propose that a symmetric phenomenon with respect to IP black holes can also exist on the Internet that of the concept of IP White Holes which will be packet generators in the internet. Now these packets can act as potential traffic congestors for the network. Many of the Denial of Service attacks including Smurf attacks, broadcast storms, packet reflector attacks etc. are by conjecture a type of White Holes on the Internet. By routing table manipulation a region of Internet can be configured by hackers to act as a packet white hole to infuse traffic on the digital backbones. Some networks by there very nature are packet white holes as they generate a lot of legitimate traffic but pose a threat to the Internet by the amount of traffic they generate. White Holes can continuously create packets on the Internet or can reroute the packets went inside a black hole to come out from the other side in the form of white holes but into a new network side. Hence IP White Holes can be a future possibility for the congestion of network traffic and potential Denial of Service attack over legitimate targets.

5. Limitations

Although the IP black hole technique is quite an effective tool in mitigating DoS and Distributed DoS attacks, it is not foolproof. The most common case where things could go wrong are:
False Alarms – For an automated scanner to decide with certitude as to “What constitutes a DoS” is highly ambiguous. There are some heuristics though, such as hosts, which get more than 10 connections from a single IP, UDP packets exceeding a pre-set rate and a surge in ICMP_ECHO replies in case of Smurf or Distributed Dos Attack. But there are systems handling heavy bandwidth applications such as multimedia streaming, DNS servers etc [2]. Noticing a surge in egress traffic an ISP scanner may be fooled into believing that the system is under a DoS attack, and hence a Black hole router may issue a false-trigger advertisement re-directing to all the packets emanating from system into a “sink”. This can effectively obviate many users from accessing services.
This is even more aggravated when the Hacker knows what Counter-measures an ISP has deployed against a DoS and Distributed Dos (they usually do) it is possible to introduce a surge of packets with the intended victim as the source IP. The Scanners are tricked into believing that the attacker is inside there own network and blacklist a perfectly legitimate system. Another problem being that if the black hole router is too promiscuous, then it puts itself as a potential DoS victim hence effectively neutralizing the network defenses.

5. Conclusion

Hence in this paper we have introduced the concept of Internet Protocol Black Holes, their existence and threat to the Internet. IP Black Holes is really a revolutionary concept and can lead to a lot of security breaches and denial of services in the future. Thus the fabric of Internet can once again be marred by so called black holes which can be deployed with ease but will be a security nightmare for the network administrators and the customers whose total business is based on the Internet. Here we see that we can take a lot of inspiration from Nature for good or bad things in the computer security world and IP Black Holes are one such bad example.

Thus we end our paper with the note that this concept of IP Black Holes and IP White Holes may become a reality some day so that we should take proactive steps rather then reactive steps to curb this monster in its bud.

6. References:

1. Inferring Internet Denial-of-Service Activity by David Moore, Geoffrey M. Voelker and Stefan Savage.
2. Wow!! that's a lot of packets at
http://www.caida.org/outreach/papers/2003/dnspackets/wessels-pam2003.pdf
3. Tracking Routing Black Holes with RIS by Dan Ardelean. (dan@ripe.net)
4 Denial of Service Attacks: Using IP Routing as a Security Tool by Brad EngStrom, Cisco Systems.
5 Black Hole Routers by Damir Rajnovic, Incident Manager, Cisco.
6 Sink Hole Deployments by Barry Raveendran Greene (bgreene@senki.org)