Anti-Spam and Cybercrime Investigation One-Page Training Series

ASNs (Autonomous System Numbers)

1. What Is An ASN?

An ASN, or Autonomous System Number, is usually technically defined as a number assigned to a group of network addresses, managed by a particular network operator, sharing a common routing policy. Most ISPs, large corporations, and university networks have an ASN. For example, Google uses AS15169, Sprint uses AS1239, Intel uses AS4983, the University of California at Berkeley uses AS25 and so on.

Some large networks with particularly complex routing policies may have more than one ASN; others, with simple routing policies and only a single upstream network provider, may have none (their network blocks are just announced using their upstream provider's ASN).

Bottom line, in general, think of an ASN as a number that "maps to" or represents a particular provider or network. As such, it is a useful way to aggregate and sort IP addresses into useful chunks, even though its initial purpose (and continued most important usage) is in conjunction with BGP4 for inter-AS routing of network traffic.

2. How Do ISPs Get An ASN?

ISPs apply to their local registry (e.g., ARIN, RIPE, APNIC or LACNIC). To be eligible to receive an ASN, the requesting organization must be able to satisfy the guidelines for issuance of an ASN, complete the required paperwork, and pay the required fee. See, for example: http://www.arin.net/policy/asn.html

Note that ASN requests typically receive careful scrutiny by the registrars because they are a scarce/key resource (there are less than 65,000 ASNs currently available for allocation Internet wide, and of that, >30,000 have already been assigned).

3. Translating Dotted Quads (IPv4 Numeric Addresses) To ASNs

While the DNS system has traditionally made it routine for users to translate a symbolic domain name to a dotted quad (or a dotted quad to a symbolic domain name), translation of a dotted quad to an ASN has traditionally required access to a router's command line interface, access which is normally limited solely to network engineers.

The network research community, however, now offers a number of publicly available route viewers that can be used for that purpose. For example, assume you wanted to know the AS number associated with MIT's web server, www.mit.edu, which currently has the IP address 18.181.0.31. You would run telnet (either from a Unix/Linux/Mac OS X terminal window, or from the Microsoft Windows command prompt (Start ==> Programs ==> Accessories ==> Command Prompt):

```
telnet route-views.oregon-ix.net
route-views.oregon-ix.net> show ip bgp 18.181.0.31
[intervening stuff snipped]
267 2914 3356 3
[additional stuff snipped]
--More-- q
route-views.oregon-ix.net> quit
```

The AS number associated with that dotted quad is the right-most value shown, in this case AS3 (MIT was obviously one of the first sites to be assigned an ASN).

That interactive process, while convenient for a small number of queries, doesn't scale well for large numbers of dotted quad to ASN queries. For large numbers of queries, it will generally be more convenient for users to query the IP-to-ASN DNS zone that has been created from the Routeviews data using the Unix host command (or dig, nslookup, etc.). When querying this zone, you **must** explicitly ask for txt type records!

```
host -t txt 31.0.181.18.asn.routeviews.org     (note reversed IP octets!)
31.0.181.18.asn.routeviews.org text "3" "18.0.0.0" "8"
```

The data returned by this sort of query includes the ASN itself (3), the origin of the network block (18.0.0.0), and the CIDR length of the encompassing block (/8).

More information about the Routeviews project is available from the Routeviews web site (http://www.routeviews.org/).

(continued)

4. What Provider Has ASN X?

To determine the provider associated with a given ASN, use whois to query whois.arin.net, whois.ripe.net, whois.apnic.net, or whois.lacnic.net, as appropriate (you may need to try each in succession):

```
whois -h whois.arin.net AS3561
OrgName: Cable & Wireless USA
[etc]
```

If your operating system doesn't include a whois client, web accessible whois services are also available via http://www.arin.net/whois/ http://www.ripe.net/whois/ http://www.apnic.net/search/ and http://lacnic.net/en/

5. Identifying the Network Address Blocks Associated with a Given ASN

Sometimes you will know a particular ASN, such as AS7018 (ATT Worldnet), and would like to know what network address blocks are being announced by that ASN. If you telnet to route-views.oregon-ix.net, you can enter the command:

```
show ip bgp regex _7018$
```

you will then be shown a list of the network blocks being routed for that ASN.

Others may prefer to use a Perl utility such as route-leecher.pl (see http://www.spamshield.org/) to extract lists of blocks.

If you prefer a web-based interface to ASN-related netblock allocation information, see: http://www.cidr-report.org/ (scroll down to "Selected AS Report") Please note that that report is based on the routing table provided from a single commercial ISP's routing table so in some cases it might not show routes for some blocks that are listed by other sources. For example, it does not show network blocks routed by AS11537 (the Internet2 Abilene network) because Abilene doesn't announce its routes to the commodity Internet.

6. Sample Simple Network Security Scenarios Involving Use of ASNs

Sample Scenario 1: Investigation of a distributed denial of service attack (or other network security event) yields a large list of hundreds (or even thousands) of IP addresses. The investigating party wishes to bring relevant IPs to the attention of suitable network security contacts — but which IP addresses belong to which ISP? Historically, the IPs might be mapped to ISPs based on domain names returned by nslookup or dig, but PTR records may be missing for many dotted quads of interest. Registry whois data for address block allocations/assignments, or Routing Asset data from whois.radb.net could also be tried, but may result in information of widely varying specificity, currency, and accuracy when it comes to the responsible parties who should be associated with a given address of interest.

Running a list of IP addresses through an IP-to-ASN conversion routine, on the other hand, allows all the dotted quads associated with that attack to be quickly mapped to their relevant parent ASN (assuming the address in question is still being announced) for reporting or other action. This is easily done a variety of different ways, including via the Team Cymru public whois server dedicated to mapping IP numbers to ASNs (see http://www.cymru.com/BGP/whois.html).

Sample Scenario 2: An entity wants to determine if a given provider is having general security issues. There are some security reporting sites which may provide reports by provider name or network block, but in most cases, the most appropriate large scale aggregation unit is the ASN. One example of a network security reporting site that's offering an experimental by-ASN security incident report is http://www.mynetwatchman.com/ListIncidentbyASSummary.asp

Sample Scenario 3: An unauthorized user hijacks a block of IP addresses, and begins using those addresses without proper authorization (because of spammer demand for un-blackholed IP space, this occurs more often than you might think — see, for example http://www.completewhois.com/hijacked/). A key issue in resolving IP address hijacking incidents is monitoring routing data to determine what provider/ASN is announcing that unauthorized block.

Sample Scenario 4: As part of resolving an incident, an investigator wants to determine what upstream ISPs (e.g., what ASNs) are providing connectivity for a blackhat ISP. Naive users might try to do this using traceroute, but traceroute from a single location fails to capture the full set of possible diverse routes that might be associated with a given ISP's connectivity. Using show ip bgp (per section 3 of this document) overcomes or at least minimizes that problem.

7. Some Additional Resources Concerning ASNs and BGP

http://www.bgpexpert.com/ (particularly excellent online resources section and book section)
http://www.bgp4.as/ (very nice site with great pointers to a variety of interesting presentations)