1 March 2007

Factsheet

Root server attack on 6 February 2007

Executive summary

- The Internet sustained a significant distributed denial of service attack, originating from the Asia-Pacific region, but withstood it.
- Six of the 13 root servers that form the foundation of the Internet were affected; two badly. The two worst affected were those that do not have new Anycast technology installed.
- The attacks highlighted the effectiveness of Anycast load balancing technology.
- More analysis is needed before a full report on what happened can be drawn up. The reasons behind the attack are unclear.
- Root server operators worked together in a fast, effective and co-ordinated effort.
- Recommendations made last year for improving the security of the DNS still need to be followed through. Other measures should also be considered.

On 6 February 2007, starting at 12:00 PM UTC (4:00 AM PST), for approximately two-and-a-half hours, the system that underpins the Internet came under attack. Three-and-a-half hours after the attack stopped, a second attack, this time lasting five hours, began.

Fortunately, thanks to the determined efforts of engineers across the globe and a new technology developed and implemented after the last DNS attack of this size, on 21 October 2002, the attack had a very limited impact on actual Internet users.

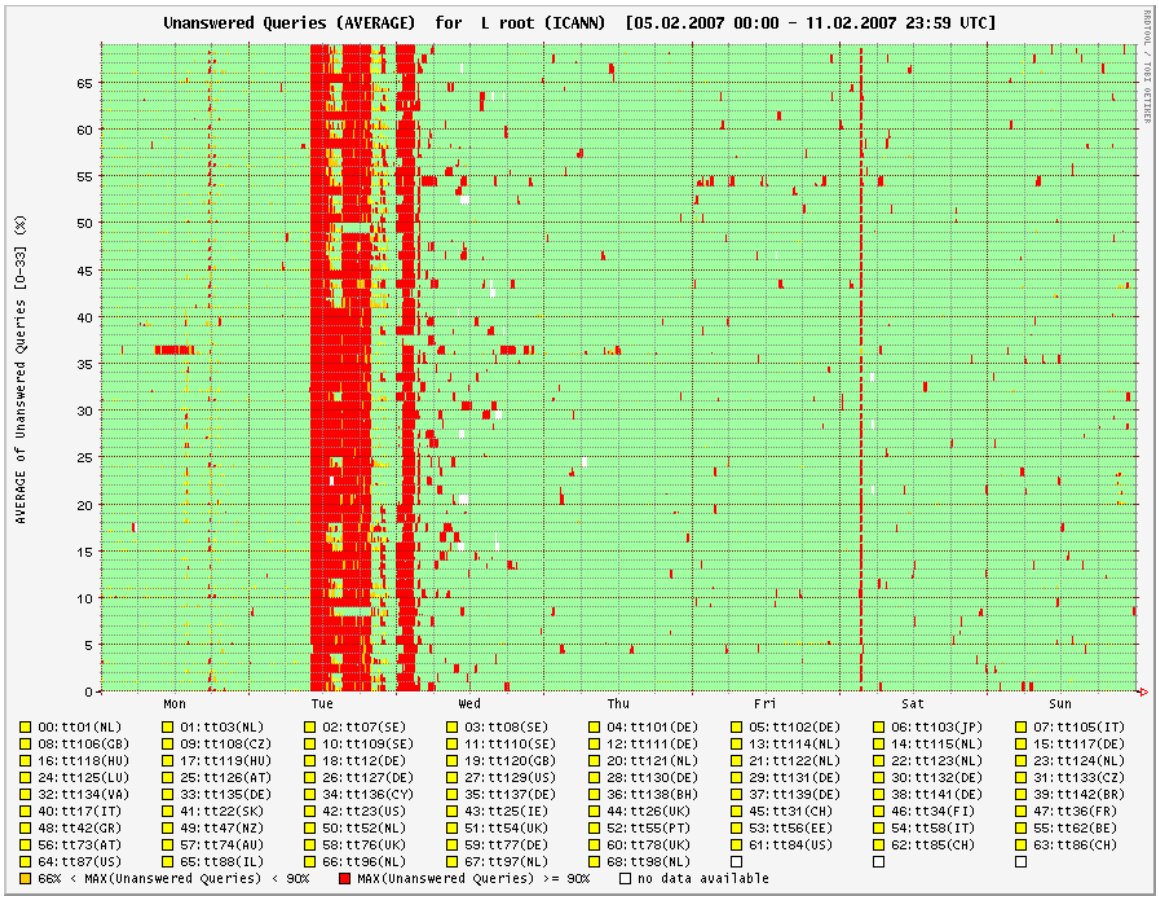
This factsheet provides the most important details of the attack and briefly explains how the domain name system works and the systems in place to protect it. It also outlines how such attacks are possible and discusses possible solutions to future attacks.

What happened?

The core DNS servers of the Internet were hit with a significant distributed denial of service attack, or DDoS. In such an attack, billions of worthless data packets are sent from thousands of different points on the Internet to specific computer servers in order to overwhelm them with requests and so disrupt the smooth running of the Internet.

The Internet works by splitting up information into very small packets, and then appending a small amount of identifiable information so that the packets can be rebuilt at the other end. This approach is what makes the Internet so effective at sharing information. However, it is both possible to create false packets and to use the Internet's checking system—which makes sure that packets aren't lost along the way—to attack a specific spot on the Internet.

It is still too early to be sure of the exact method used—a meeting of root server operators in March will hope to gain a better understanding—but so far there are two broad conclusions: the attack originated from the Asia-Pacific region and the Anycast technology that was designed to deal with such attacks worked very effectively.



The attack on L-root in the week of 5 February 2007 (source: RIPE NCC dnsmon)

At least six root servers were attacked but only two of them were noticeably affected: the "g-root", which is run by the U.S. Department of Defense, and the "l-root" run the Internet Corporation for Assigned Names and Numbers (ICANN), based in California.

The reason why these two were particularly badly affected was because they are the only root servers attacked that have yet to install Anycast (a further three root servers without Anycast were not attacked this time).

Even though it was a large attack, the new technology, combined with the speed, skills and experience learnt by root server operators over the years, helped to make sure that actual Internet users were not inconvenienced.

What are root servers and why are there only 13 of them?

Root servers are the base on which the Internet's naming system runs. Each server contains a copy of the same file, refreshed and replaced twice a day, which lists where on the Internet all the directories for top-level domains such as .com or .net or .uk can be found. The file itself is actually very small but it acts as the Net's definitive directory and without it, the single Internet that we enjoy now would be put at risk.

There are 13 servers dotted across the world that store this file (and they are named "A" through to "M"). The reason why there are 13 is due to the decision back in the very early days of the Internet to give a certain type of data packet (called UDP) a maximum size of 512 bytes. This 512-byte size provides just enough room to name 13 different places on the network (although they are represented by servers in more than 100 different places geographically).

Although it has since become possible to send much larger UDP packets, the speed, simplicity and universal acceptance of the 512-byte UDP packet has meant that retaining 13 root servers has been agreed on as the most secure way to underpin the Internet.

In theory, if even one of the 13 root servers is up and running then the Internet will continue to run unhindered as the directory will still be visible to the network. This theory was put to the test in October 2002 when an attack similar to the one in early February 2007 managed to swamp nine of the 13 servers. The Internet continued to run but it was a wake-up call for the

root server operators who immediately set about devising a system to improve stability.

The result was the roll-out of a new technology called Anycast. Anycast allows a number of servers in different places to act as if they are in the same place. So while there remain 13 locations on the network for root servers, the reality on the ground is that not only are there often dozens at one spot but dozens of servers in other locations that can also deal with requests. In the case of the f-root, there are no less than 42 different locations supporting the root server. This approach has two advantages:

1. The servers spread the load of an attack among themselves.
2. The servers can be spread geographically around the world so if something physically happens at one location—for example an earthquake—then the root server itself can remain operational.

What do you actually do when hit with a massive attack?

The operators of the servers that were hit by the attack were aware of it almost instantaneously. Because of the way the attack worked (where a command is given at the same time to a large number of computers to send data to the same place), it arrived like a brick wall, which immediately set off all the alarms built into the networks.

Engineers looked at the statistics for their servers and made a provisional decision over what the problem was. In this case it was clear almost immediately that it was a distributed denial of service attack.

There are two main ways to deal with such an attack: either try to suck up the queries by adding extra bandwidth and servers to the system to answer all the requests and so allow more legitimate queries through; or find patterns in the queries being sent and decide if those patterns can be used to filter the attacking traffic, either by stopping the source of the attack (by ignoring all requests from it) or working with those further upstream to filter their bad traffic.

Engineers in charge of the affected servers across the world used both methods at the same time, while also talking to one another and discussing methods to remove the bad data without affecting the legitimate information that continues to flow at the same rate as normal over the network.

In the case of an attack in February of 2006, engineers soon discovered that all the attack packets were larger than the 512-byte size and so simply blocked any packets larger than that. Since most typical data packets are actually less than 100 bytes in size, the effect of stopping larger packets had virtually no impact on normal Internet users but managed to kill the attack, which at that point accounted for 99.7 percent of all the traffic in the system.

Root server operators have a wide range of emergency communication procedures in place, from established protocols and connections to secure chatrooms, right down to home telephone numbers of the most senior engineers, enabling them to share data and offer help. Data can then be compiled and analysed to learn from an incident and evaluate performance.

What do you mean by queries?

This is a highly simplified but illustrative explanation of how the Internet works: you type in a domain name or a search term and your computer tries to find where in the world the information that relates to that data is. That data can in fact be anywhere on any computer anywhere in the world so long as it is connected to the Internet, so finding it requires a highly efficient address book.

The domain name system is that address book, translating easy-to-remember names into the harder-to-remember numbers that computers use as addresses.

When you type a domain name into a computer, such as "www.example.com", your computer will ask (query) a known DNS server—usually provided by your ISP—for the number address of that site, called an IP address. If that server does not already know the answer, then it will enquire of the nearest matching name server that it knows. Even if it does not know anything about example.com, or even .com, all name servers know the addresses of the 13 root servers.

Those root servers contain pointers to all top-level domains, such as .com or .org or .info. The servers for .com will then know the information pointing to the name servers for example.com, which in turn will be able to answer with the IP address of www.example.com.

All this happens extremely quickly and it is all based around a system where one server is able to query another. So when attackers try to stop a server from working, they simply send millions of requests per second for information in an effort to overwhelm the server.

The attacks can be enormous. In both the attack this February and the one last February, the amount of data being sent to specific servers was measured in some cases at 1Gb per second—which is roughly equivalent to receiving 13,000 emails every second, or over 1.5 million emails in just two minutes.

Where did it come from?

All that is known at present is that the attack traffic (data packets) came from the Asia-Pacific region. There was some speculation in the press that the attack originated from South Korea. This was educated guesswork since it is likely the attack originated from hundreds of individual computers that have been infected with a virus and controlled remotely by an attacker to send data packets to a specific location.

Compromised computers—commonly called "zombies"—are combined to form "botnets" which can then be directed as required. Botnets are most commonly created by conning ordinary consumers into opening something on their computer that appears to do nothing but which installs hidden software to be used later for an attack.

Because of the widespread availability of high-speed, always-on Internet access in South Korea, those seeking to create botnets from across the world often target citizens in the country as it is likely to yield a higher success rate. But while the logic may appear to be firm, the data is so far inconclusive as to where the attack came from.

It could just as easily have come from a number of different countries at the same time. It is even possible that the attack originated from outside the region and many of the Internet addresses that the attack appeared to come from had in fact been "spoofed" or faked. In fact, engineers are fairly sure that it did come from Asia-Pacific, but even so this does not mean that whoever was behind the attack is based in Asia-Pacific because they could just as easily triggered it from anywhere on the network, i.e., anywhere in the world.

Why aren't all root servers using Anycast if it's so good?

This was in fact a conscious decision on the part of the root server operators. Common practice among Internet engineers across the globe is to make sure that the systems they use vary so that there is no single point of failure.

For example, many of the normal DNS servers that companies and even individuals run are built on top of Windows, but others are on Linux, some are on MacOS X, some are on NetWare, Unix, OS/2 and so on. They also use different software and different versions of the same software. Why? Because if everyone ran the same software on the same operating system, there is the risk that a specific security hole could take down the whole system. Running a wide variety hugely reduces that risk.

So it was with the Anycast system. There were some concerns that there might be a security risk in allowing a lot of different servers to appear as if they were coming from the same place. And so just a few root servers tried the system first, tested it thoroughly and ironed out any bugs before the next set moved over.

With the Anycast technology apparently proven, it is likely that the remaining roots—D, E, G, H and L—will move over soon.

Where are the root servers?

Due to the Internet's historical basis, nine of the 13 root servers were originally based in the United States (with four in California). The four outside the US were based in Japan, the Netherlands, Sweden and the UK. However, with Anycast technology the situation has changed dramatically and now there are more root servers based outside the United States than within it. You can find, in total, over 100 root servers on every continent and in countries ranging from Australia to Venezuela.

Do the root server operators talk to one another?

Yes. While each operator retains a large degree of autonomy, the operators meet regularly at Internet conferences. Most of the operators know one another personally and have developed close working relationships.

Over the years, the operators have developed a series of procedures and protocols to aid them in their work. Aside from having the contact details for server locations, they also have home telephone numbers of individual engineers in case of an emergency. When an attack does appear, multiple lines of secure communication are prepared, including telephones, chatrooms and instant messaging.

The group will then largely work together as a team, sharing information and identifying the problem areas. Those operators that are either not included in the attack or whose servers are holding up will offer their assistance, whether that be in analysing trends or reconfiguring equipment to help stave off the attack.

Who's in charge of co-ordinating the root servers?

No one person or group is in charge of the servers or of co-ordinating their operators, although there are two committees that exist within the Internet Corporation for Assigned Names and Numbers (ICANN) that often review the situation and provide advice and occasional recommendations about the operational requirements of root name servers and their security. They are the Root Server System Advisory Committee (RSSAC) and the Security and Stability Advisory Committee (SSAC).

The RSSAC usually meets during IETF (Internet Engineering Task Force) meetings, and the SSAC usually meets during ICANN meetings.

Why do people attack the root servers anyway?

People's motives for attacking a system that they have clearly dedicated years to understanding is uncertain. It is widely believed that attacks on the domain name system are simply a result of the hacker mentality directed at a different target.

The technical challenge associated with bringing down some of the world's most heavily protected servers is certainly one explanation. The desire to say that you brought down the Internet is something that is likely to inspire a small group of individuals.

However, while it remains quite rare that the root servers themselves are attacked, there is a long history of people using the same techniques to target individual websites, sometimes for personal reasons, sometimes for political reasons, sometimes for financial gain.

More recently, with the expansion of e-commerce, denial of service attacks are being used by criminal gangs as a form of extortion. Gambling sites and banks have occasionally been the target of disruptive attacks and asked to provide payment in return for ending them. This in itself has created a market for botnets which can be hired or purchased from the individuals who have built them in order to direct an attack.

One possible explanation for the root server attacks is that they act as an advertisement for a particular botnet.

What can be done to reduce the risk of such attacks in future?

There are various measures aside from strengthening the root servers that will aid in defeating future attacks on the DNS.

In a March 2006 report on the DNS attack of the previous month, the SSAC made three recommendations for counteracting such attacks:

1. That those running networks adopt "source IP address verification"—i.e., that they improve and tighten existing systems.
2. That root server operators—and those running country code top-level domains—draw up their countermeasure policies, respond quickly to queries, and act quickly to add servers back into the system if the owner shows they have improved their security.
3. ISPs should only accept DNS queries from trusted sources (i.e., their own customers) rather than allow anyone to use their servers.

Those recommendations have met with mixed success: the problem in many cases is that there is nothing beyond a moral sense of obligation to push the changes through. In many cases, the cost of reviewing and reconfiguring systems has seen the issue put on the back burner.

Aside from the infrastructural changes, there is the issue of botnets and individual behaviour. Operating system manufacturers—Microsoft in particular—have invested heavily in recent years in improving the security of their software so it is harder for people to remotely take over machines. However, it is also vital that individual Internet users are educated to recognise what is likely to be an effort to secretly install software on their home computers.

A third category is the huge increase in individual Internet users installing routers in their homes, usually to provide wireless access or to link up several computers in the house. These consumer products usually come with the same password and a large percentage of home users never change this default password, making it easy for hackers to seize control of them for their own ends. If consumers were encouraged to change the default password or if router manufacturers were persuaded to provide each unit with a different password, then future attacks against the Net's infrastructure could be tackled at the source.

Where can I find more information?

Wikipedia article on Anycast:
http://en.wikipedia.org/wiki/Anycast

The owners of the f-root discuss Anycast:
http://www.isc.org/index.pl?/pubs/tn/?tn=isc-tn-2003-1.html

Wikipedia article on root servers:
http://en.wikipedia.org/wiki/Root_nameserver

The Root Servers Association:
http://www.root-servers.org/

Root Server System Advisory Committee:
http://www.icann.org/committees/dns-root/

Security and Stability Advisory Committee:
http://www.icann.org/committees/security/

SSAC report into February 2006 attack:
http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf

RIPE NCC's dnsmon monitoring service:
http://dnsmon.ripe.net/dns-servmon/

Useful Terms

Anycast – A network addressing and routing scheme whereby data is routed to the nearest or best destination as viewed by the routing topology. In anycast, there is also a one-to-many association between network addresses and network endpoints: each destination address identifies a set of receiver endpoints, but only one of them is chosen at any given time to receive information from any given sender. Anycast is best suited to connectionless protocols rather than connection-oriented protocols such as TCP, since the receiver selected for any given source may change from time to time as optimal routes change, silently breaking any conversations that may be in progress at the time. Anycast is generally used as a way to provide high availability and load balancing for stateless services such as access to replicated data; for example, DNS service is a distributed service over multiple geographically dispersed servers.

botnet – Compromised computers, or "zombies", are combined to form "botnets" which can then be directed as required. Botnets are most commonly created by conning ordinary consumers into opening something on their computer that appears to do nothing but which installs hidden software to be used later for an attack.

Distributed denial of service attack, or DDoS – A type of denial of service attack in which an attacker uses malicious code installed on various computers to attack a single target. An attacker may use this method to have a greater effect on the target than is possible with a single attacking machine. On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. DDoS attacks are most effective when launched via a large number of open recursive servers: distribution increases the traffic and decreases the focus on the sources of the attack. The impact on the misused open recursive servers is generally low, but the effect on the target is high. The amplification factor is estimated at 1:73. Attacks based on this method have exceeded seven (7) Gigabits per second.

Domain Name System – The domain name system (DNS) helps users to find their way around the Internet. Every computer on the Internet has a unique address—just like a telephone number—which is a rather complicated string of numbers. It is called its "IP address" (IP stands for "Internet Protocol"). IP addresses are hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters (the domain name) to be used instead of the arcane IP address. So instead of typing 207.151.159.3, you can type www.internic.net. It is a mnemonic device that makes addresses easier to remember. The DNS translates the domain name you type into the corresponding IP address, and connects you to your desired website. The DNS also enables email to function properly, so the email you send reaches the intended recipient.

ICANN – The Internet Corporation for Assigned Names and Numbers is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) top-level domain name system management and root server system management functions. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes.

RSSAC – The Root Server System Advisory Committee advises the ICANN community and Board about the operation of the root name servers of the domain name system. It also provides advice on the operational requirements of root name servers, including host hardware capacities, operating systems and name server software versions, network connectivity and physical environment. RSSAC examines and advises on the security aspects of the root name server system, and reviews the number, location, and distribution of root name servers considering the total system performance, robustness, and reliability.

SSAC – The Security and Stability Advisory Committee advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services such as Whois). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly.

About ICANN

ICANN is a nonprofit organisation responsible for coordinating the Internet's systems of unique identifiers, including the systems of domain names and numeric addresses that are used to reach computers and other devices on the Internet. ICANN's mission is to ensure the stable and secure operation of these unique identifier systems, which are vital to the Internet's operation. In addition, ICANN coordinates policy development related to these technical functions through its effective bottom-up consensus model. Further information about ICANN is available at http://icann.org.

ICANN

4676 Admiralty Way, Suite 330, Marina del Rey, CA 90292 USA
+1 310 823 9358 tel +1 310 823 8649 fax

6 Rond Point Schuman, Bt. 5, B-1040 Brussels Belgium
+32 2 234 7870 tel +32 2 234 7848 fax

CA_bw_0703 v1.1