When the Internet goes down

March 2 2018, by Hervé Debar

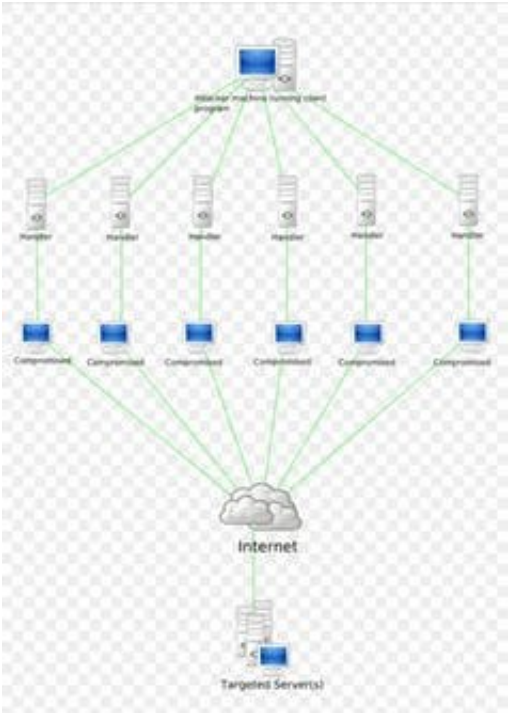

Diagram of a denial-of-service attack. Credit: Everaldo Coelho and YellowIcon, CC BY

"A third of the Internet is under attack. Millions of network addresses were subjected to distributed denial-of-service (DDoS) attacks over two-year period," reports Warren Froelich on the UC San Diego News Center website. A DDoS is a type of denial-of-service (DoS) attack in which the attacker carries out an attack using many sources distributed throughout the network.

But is the journalist justified in his alarmist reaction? Yes and no. If one-third of the Internet was under attack, then one in every three smartphones wouldn't work, and one in every three computers would be offline. When we look around, we can see that this is obviously not the case, and if we now rely so heavily on our phones and Wikipedia, it is because we have come to view the Internet as a network that functions well.

Still, the DDoS phenomenon is real. Recent attacks testify to this, such as the attack by the botnet Mirai on the French web host OVH and the American web host DynDNS. The websites owned by customers of these servers were unavailable for several hours.

What the source study really looked at was the appearance of IP addresses in the traces of DDoS attacks. Over a period of two years, the authors found the addresses of two million different victims, out of the 6 million servers listed on the web.

Traffic jams on the information superhighway

Units of data, called packets, circulate on the Internet network. When all of these packets want to go to the same place or take the same path, congestion occurs, just like the traffic jams that occur at the end of a workday.

It should be noted that in most cases it is very difficult, almost impossible, to differentiate between normal traffic and denial of service attack traffic. Traffic generated by "flash crowd" and "slashdot effect" phenomena is identical to the traffic witnessed during this type of attack.

However, this analogy only goes so far, since packets are often organized in flows, and the congestion on the network can lead to these packets being destroyed, or the creation of new packets, leading to even more

congestion. It is therefore much harder to remedy a denial-of-service attack on the web than it is a traffic jam.

This type of attack saturates the network link that connects the server to the Internet. The attacker does this by sending a large number of packets to the targeted server. These packets can be sent directly if the attacker controls a large number of machines, a botnet.

Attackers also use the amplification mechanisms integrated in certain network protocols, such as the naming system (DNS) and clock synchronization (NTP). These protocols are asymmetrical. The requests are small, but the responses can be huge.

In this type of attack, an attacker contacts the DNS or NTP amplifiers by pretending to be a server that has been attacked. It then receives lots of unsolicited replies. Therefore, even with a limited connectivity, the attacker can create a significant level of traffic and saturate the network.

There are also "services" that offer the possibility of buying denial of service attacks with varying levels of intensity and durations, as shown in an investigation Brian Krebs carried out after his own site was attacked.

What are the consequences?

For Internet users, the main consequence is that the website they want to visit is unavailable.

For the victim of the attack, the main consequence is a loss of income, which can take several forms. For a commercial website, for example, this loss is due to a lack of orders during that period. For other websites, it can result from losing advertising revenue. This type of attack allows an attacker to use ads in place of another party, enabling the attacker to tap into the revenue generated by displaying them.

There have been a few, rare institutional attacks. The most documented example is the attack against Estonia in 2007, which was attributed to the Russian government, although this has been impossible to prove.

Direct financial gain for the attacker is rare, however, and is linked to the ransom demands in exchange for ending the attack.

Is it serious?

The impact an attack has on a service depends on how popular the service is. Users therefore experience a low-level attack as a nuisance if they need to use the service in question.

Only certain large-scale occurrences, the most recent being the Mirai botnet, have impacts that are perceived by a much larger audience.

Many servers and services are located in private environments, and therefore are not accessible from the outside. Enterprise servers, for example, are rarely affected by this kind of attack. The key factor for vulnerability therefore lies in the outsourcing of IT services, which can create a dependence on the network.

Finally, an attack with a very high impact would, first of all, be detected immediately (and therefore often blocked within a few hours), and in the end would be limited by its own activities (since the attacker's communication would also blocked), as shown by the old example of the SQL Slammer worm.

Ultimately, the study shows that the phenomena of denial-of-service attacks by saturation have been recurrent over the past two years. This news is significant enough to demonstrate that this phenomenon must be addressed. Yet this is not a new occurrence.

Other phenomena, such as routing manipulation, have the same consequences for users, like when Pakistan Telecom hijacked YouTube addresses.

Good IT hygiene

Unfortunately, there is no sure-fire form of protection against these attacks. In the end, it comes down to an issue of cost of service and the amount of resources made available for legitimate users.

The "big" service providers have so many resources that it is difficult for an attacker to catch them off guard.

Still, this is not the end of the Internet, far from it. However, this phenomenon is one that should be limited. For users, good IT hygiene practices should be followed to limit the risks of their computer being compromised, and hence used to participate in this type of attack.

It is also important to review what type of protection outsourced service suppliers have established, to ensure sure they have sufficient capacity and means of protection.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation