What is a smurf attack?

Smurf attacks are a subcategory of the DDoS attacks. They are based on the smurf malware - from where the name also appeared. According to [1] smurf attacks are amplification vectors, which boosts the damage potential by abusing the weakness of a broadcast network. It is easy to accidentaly get the smurf malware, according to [2] a smurf trojan, from infected sources. The malware is hidden until activated by a remote user. Because it is “sleeping”, it can have bundle of rootkits, which allow the hacker to open backdoors in the infected system. Sometimes a smurf attack, if successfull, cripples the system from hours to days, and can cover more sinister scenarios where files and information are stolen.

In [1] a smurf attack scenario is exemplified:

Smurf malware is used to generate a fake Echo request containing a spoofed source IP, which is actually the target server address.

The request is sent to an intermediate IP broadcast network.

The request is transmitted to all of the network hosts on the network.

Each host sends an ICMP response to the spoofed source address

With enough ICMP responses forwarded, the target server is brought down.

Important to know is, that the more hosts there are the more powerful the attack is, that because the amplification factor is correlated to the number of hosts [1].

Another source, [3], defines that a smurf attack can be divided in two categories:

The basic attack: where the victim is in the middle of the ICMP request packet flood. If the packets disperse correctly, then every device that connects to the network would reply to the ICMP request. This leads to the bandwidth beeing “eaten”, resulting in a lot of traffic and destroying in the end the system.

Another type is the advanced attack: it starts like the basic attack, but it sends the responds to a third-partie victim. This means the hackers slow down a larger part of the network, as what they would manage to achieve with only one victim.

How to combat a smurf attack?

One way is to turn off the IP broadcast adressing on the network router. It is a function which is rarely used, and if is turned off is makes it impossible for the hacker to overwhelm the network. Same as with other DDoS attacks, a robust prevention method is needed to monitor and detect anomalies.

The smurf attack sounds like a childrens cartoon, but it poses real threat if the servers / networks are overwehlmed. The most important protective measures, according to [2], are to make sure the directed broadcast traffic is blocked and to set the hosts and routers to not respond to ICMP echo requests.