What is a Smurf Attack?

usa.kaspersky.com/resource-center/definitions/what-is-a-smurf-attack

April 20, 2022

SECURITY DEFINITION

A Smurf attack is a form of a distributed denial of service (DDoS) attack that renders computer networks inoperable. The Smurf program accomplishes this by exploiting vulnerabilities of the Internet Protocol (IP) and Internet Control Message Protocols (ICMP).

The steps in a Smurf attack are as follows:

- First, the malware creates a network packet attached to a false IP address — a technique known as "spoofing."
- Inside the packet is an ICMP ping message, asking network nodes that receive the packet to send back a reply
- These replies, or "echoes," are then sent back to network IP addresses again, setting up an infinite loop.

When combined with IP broadcasting — which sends the malicious packet to every IP address in a network — the Smurf attack can quickly cause a complete denial of service.

Smurf Attack Transmission and Effects

It's possible to accidentally download the Smurf Trojan from an unverified website or via an infected email link. Typically, the program will remain dormant on a computer until activated by a remote user; as a result, many Smurfs come bundled with rootkits, allowing hackers to create backdoors for easy system access. One way to combat a Smurf attack is to turn off IP broadcast addressing on every network router. This function is rarely used, and if turned off it is not possible for the attack to overwhelm a network.

If a Smurf DDoS attack does succeed, it can cripple company servers for hours or days, resulting in lost revenue and customer frustration — what's more, this kind of attack may also be a cover-up for something more sinister, such as theft of files or other intellectual property (IP). Dealing with Smurf and similar DDoS attacks requires a robust prevention strategy that is able to monitor network traffic and detect any oddities, for example packet volume, behaviour and signature; many malware bots exhibit specific characteristics, and the right security service can help shut down a Smurf or other DDoS attack before it begins.

How to Protect Yourself

The Smurf Attack sounds cute but poses real risks if servers are overwhelmed. Disabled IP broadcasting and reliable detection tools help limit the chance and impact of this attack. Here are a couple of steps to for Smurf attack mitigation:

- make sure to block directed broadcast traffic coming into the network
- configure hosts and routers not to respond to ICMP echo requests.

A variation to the Smurf attack is the Fraggle attack. The attack is essentially the same as the Smurf attack but instead of sending an ICMP echo request to the direct broadcast address, it sends UDP packets. For the Fraggle attack, it is the same mitigation process.