BlackNurse

What is BlackNurse?

BlackNurse is a non-volumetric**,** low bandwidth Denial-of-Service attack that overloads firewalls and can potentially knock businesses offline. It can be easily launched from a single laptop.

How Does it Work?

Most ICMP attacks that Radware witnesses are based on ICMP Echo (Type 8 Code 0) and are called ping flood attacks. These attacks deny the service via excessive bandwidth and filling up internet pipes.

The BlackNurse attack targets a vulnerability in some network and security devices, fire walls mainly. The attack can be triggered with a limited volume of 15-18Mbps of ICMP Type 3 Code 3 or about 40k to 50k packets per second (PPS). The impact on these network and security devices is typically high CPU loads causing the devices to stop forwarding packets or creating new sessions. When the attack stops, most devices will recover to normal condition.

Why is it Effective?

Typically, firewalls are setup to block a subset of ICMP. Most security best practices indicate to block ping and traceroute: ICMP type 0 (echo reply), 8 (echo request) and 11 (time exceeded). These are only 3 out of the 16 ICMP types. Some others types like 4 (source quench) and 3 (destination unreachable) are required for keeping hosts operating properly on a network. One such example is Path MTU discovery, which requires the destination unreachable, don't fragment bit set message (type 3, code 4)

According to RFC 1812 - Requirements for IPv4 Routers, a router MUST be able to generate ICMP Destination Unreachable messages and SHOULD choose a response code that most closely matches the reason the message is being generated.

Advisory to Radware Customers:

Radware security professionals have tested BlackNurse attack against our attack mitigation solutions - the behavioral denial of service (BDOS) analysis engine successfully detected the attack and mitigated it, generating a signature to block BlackNurse packetflood.

In addition, specific signatures have been put in place to update all DefensePro's installations. Radware's Emergency Response Team is fully aware of the BlackNurse threat and is available 24x7 to address any attack.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under a DDoS attack or malware outbreak and in need of emergency assistance, **Contact us**.