Black Nurse - DDoS technology makes it possible for a normal laptop to take down a server as well

Even if those servers are equipped with well-known firewall devices, they can still be knocked out if the attacker exploits this technique.

Even if those servers are equipped with well-known firewall devices, they can still be knocked out if the attacker exploits this technique.

It may sound unbelievable, but instead of a giant botnet, you only need a laptop with an Internet connection to launch a powerful **DDoS** attack, take down important Internet servers and show firewalls. great.

Researchers at the TDC Security Operations Center have discovered a new attack technique that allows single attackers with limited resources (in this case, a laptop with a network of tapes). bandwidth with at least 15 Mbps) can **take down** large **servers** .

Dubbed **BlackNurse - Black Nurse attack technique** or **low speed " *Ping of Death* " attack** , this technique can be used to launch a series of low-volume DoS service denial attacks. How to send ICMP packets or "ping" to flood the processor on the server.

Even servers protected by **firewalls from Cisco** , **Palo Alto Networks** , or other companies are also affected by this attack technique.

ICMP (Internet Control Message Protocol) is a protocol used by routers and other network devices to send and receive error messages.

Ping of Death is an attack technique that overloads the network by sending ICMP packets in excess of 65,536 bytes to the target. Because this size is larger than the allowable size of IP packets, it will be broken down and then sent partially to the destination host. Upon reaching the target, it will be reassembled into a complete packet, due to its excessive size, it will cause buffer overflow and hang.

According to a technical report released this week, the technique to attack BlackNurse is also known under a more traditional name: " *attack to cause ping flood* " and it is based on ICMP Type 3 queries (or errors). Destination Unable to access - Destination Unreachable) Code 3 (Port Unreachable error).

These queries are replies, usually returning ping sources when the destination port of the target is inaccessible - or **Unreachable** .

1. Here's how the BlackNurse attack technique works:

By sending a **Type 3 ICMP** packet with a code of 3, a hacker can cause a denial of service (DoS) by overloading CPUs on certain types of server firewalls. , no matter what the quality of the Internet.

BlackNurse technical access is very small, only from 15 Mbps to 18 Mbps (or between 40,000 and 50,000 packets per second), especially when compared to a record 1 Tbps DDoS attack targeting a provider OVH French Internet service in September.

Meanwhile, TDC also said that this huge volume is not an important issue when just maintaining a steady stream of ICMP packets from 40K to 50K to the victim's network device is destructive. target device.

So what is the good news here? " *When the attack takes place, users on the LAN will not be able to send or receive access to and from the Internet anymore. All the firewalls that we have seen are recovering later," the researchers said. when the attack stops* . "

However, this means that this low-volume DoS attack technique is still very effective because it not only floods the firewall with access, but also forces the CPU to load at a high level, even Take down offline servers if the attack has enough network capacity.

Researchers believe **BlackNurse** should not be confused with attacks that cause ping flooding based on ICMP Type 8 Code 0 packets (or regular ping packets). The researchers explained:

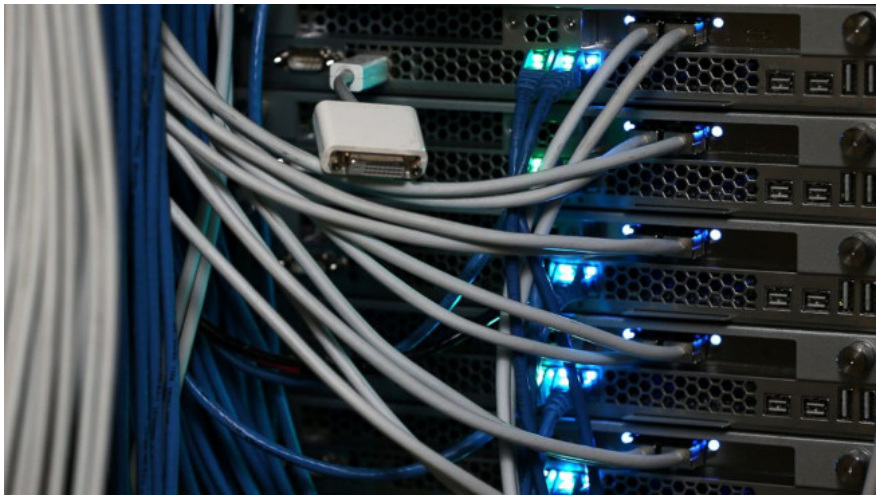
" *The BlackNurse attack technique caught our attention because in the anti-DDoS solution test, even if the access rate and packet volume per second were very low, this attack can also stop all activities of our customers* . "

" *Even this attack technique can be applied to businesses that are equipped with firewalls and have large Internet connections. We hope that professional firewall devices will be able to handle these. this attack* . "

2. The device is affected

BlackNurse attack technique is effective with the following products:

1. Firewall device Cisco ASA 5506, 5515, 5525 (at the default settings).
2. Cisco ASA 5550 (old) and 5515-X firewall devices (latest generation).
3. Cisco Router 897 (may be slightly reduced).
4. SonicWall (misconfiguration can be changed and mitigated).
5. Some unspecified equipment from Palo Alto.
6. Zyxel NWA3560-N Router (wireless attack from internal LAN).
7. Zyxel Zywall USG50 firewall device.



3. How to mitigate the BlackNurse attack?

There is still good news for you - there are several ways to counter BlackNurse attacks.

TDC offers a number of mitigation measures and **IDS SNORT** rules (**SNORT** open source intrusion detection system) that can be used to detect BlackNurse attacks. Furthermore, the PoC code (proof-of-concept) has been posted on GitHub by OVH engineers, which can also be used to test network administrators' devices against BlackNurse.

To mitigate BlackNurse attacks on firewalls and other devices, TDC recommends that users **create a list of reliable sources, be allowed to send and receive ICMP packets** . However, the best way to mitigate the attack is to simply disable the ICMP Type 3 Code 3 packet on the WAN interface.

Palo Alto Networks also released a statement, saying its devices are only affected by " *very specific scenarios, not in default settings and contrary to common practices* ." The company also listed some recommendations for its customers.

Meanwhile, Cisco said it did not assume that the behavior in the report was a security issue, but warned that:

" *We recommend that people set up licenses for packets that cannot access ICMP Type 3. Deny messages that cannot access ICMP help disable Path MTU Discovery protocol for ICMP packets. can prevent IPSec (Internet Protocol Security: a set of protocols for securing communications) and PPTP protocol access (Point-To-Point Tunneling Protocol: A protocol used to transfer data between VPN virtual private networks)* . "

Furthermore, independent software vendor NETRESEC also published a detailed analysis of BlackNurse entitled " *Attack techniques that flooded back in the 1990s have returned* ." In addition to the above warnings, Sans Institute also announced a short memo about BlackNurse's attack, discussing the attack and what users should do to mitigate it.