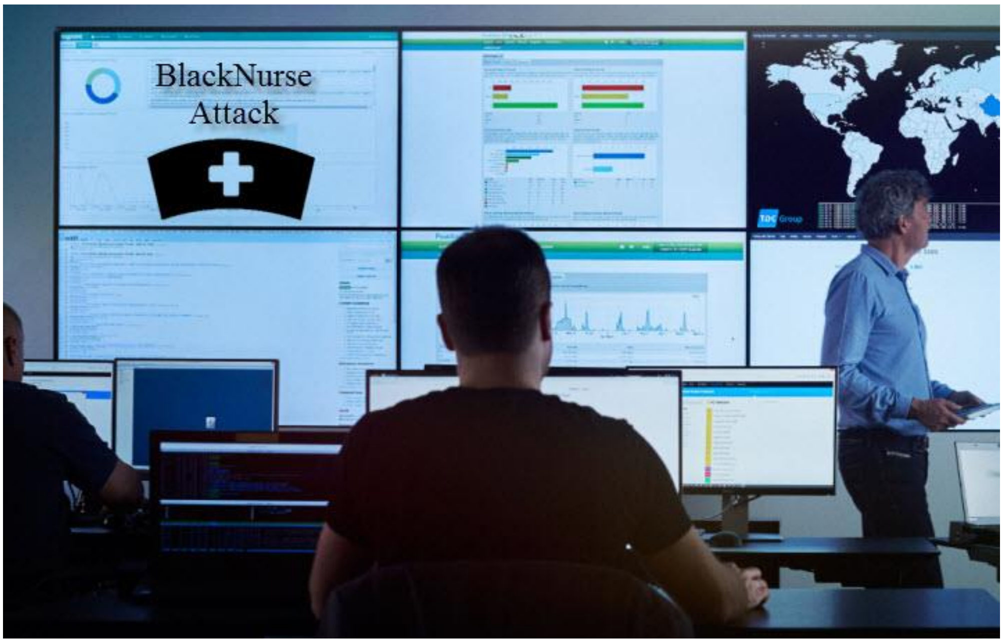
The BlackNurse Attack



Version	**1.7**
Dato	**8. November 2016**
Classification	TLP: AMBER TLP:WHITE - From 10. November 2016
Traffic Light Protocol – TLP information	http://www.first.org/global/sigs/tlp
Work performed by	TDC Group A/S – TDC SOC
Involved	Lenny Hansson – TDC SOC Per Høgh – TDC SOC Bjarne Bachmann – TDC SOC Kenneth B. Jørgensen Dennis Rand
Web-Site	Information will be public available from 10. November 2016 on the following web-site: http://soc.tdc.dk/blacknurse/blacknurse.pdf

[TDC SOC]

About TDC Security Operations Center

TDC Security Operations Center (SOC) was established in 2011 in relation to TDC's launch of TDC DoS Protection, the product that protects business customers against DDoS attacks. In 2015, TDC SOC was moved to the next level and now protects business customers against all types of cyber threats and attacks.

Facts about TDC SOC:

- The Security Operations Center is located in Copenhagen
- All employees are security cleared by the Danish authorities
- TDC SOC handles security incidents for TDC and TDC's customers
- TDC SOC is authorised to use the registered trademark 'CERT'
- TDC SOC is accredited by Trusted Introducers
- TDC SOC delivers 24/7/365 incident response

Pivotal for the operation of TDC SOC is the use of intelligence feeds from sources like:

- Malware analysis
- TDC's honeynet
- TDC core infrastructure
- TDC security products
- National and international collaboration fora
- Third-party feeds (both open source and commercial)

Prevention Detection Containment Recovery Analysis

Introduction

In TDC SOC, we handle an anti-DDoS solution for a large number of customers. We analyse all incoming DoS/DDoS attacks targeting our customers.

To be able to defend against different kinds of DoS/DDoS attacks, it is important for us and our customers that all DoS/DDoS attacks are carefully analysed. This is done so that the impact on our customers and our network is kept to a minimum. Based on the analysis, signatures are used in our anti-DDoS mitigations.

Normally with DDoS attacks, they are based on pure volume of traffic from the attacker. The pure volume of traffic is flooding the Internet connections, and thereby denying services of any kind.

As a result of one of our analyses, we have noticed that one attack form is based on the ICMP protocol. This attack is not based on pure flooding of the internet connection, and we have named it 'BlackNurse'. BlackNurse is **not** the same as an old ICMP flood attack which is known to send ICMP requests to the target very quickly. BlackNurse is based on ICMP with Type 3 Code 3 packets.

From mid-2014 until mid-2016, we have seen 95+ ICMP based attacks targeted at our customers in the TDC network. So ICMP based attacks in general are a well-known attack type used by some DDoS attackers.

The BlackNurse attack attracted our attention, because in our anti-DDoS solution we experienced that even though traffic speed and packets per second were very low, this attack could keep our customers' operations down. This even applied to customers with large internet uplinks and large enterprise firewalls in place. We had expected that professional firewall equipment would be able to handle the attack.

We know of some vendors that experience problems with BlackNurse attacks and this affects our customers. There could be more vendors affected by BlackNurse, but at this point we do not know. We have, however, worked closely with different vendors to get the information out.

We have made a survey in the Danish IP address space based on already published data, and we found that there were more than 1.7 million devices responding to ICMP ping. This could result in BlackNurse having a high impact, especially due to the potentially high impact of this attack at low bandwidths on equipment which handles ICMP poorly.

The Attack

Most ICMP attacks that we see are based on ICMP Type 8 Code 0 also called a ping flood attack. As stated earlier, BlackNurse is based on ICMP with Type 3 Code 3 packets. We know that when a user has allowed ICMP Type 3 Code 3 to outside interfaces, the BlackNurse attack becomes highly effective even at low bandwidth. Low bandwidth is in this case around 15-18 Mbit/s. This is to achieve the volume of packets needed which is around 40 to 50K packets per second. It does not matter if you have a 1 Gbit/s Internet connection. The impact we see on different firewalls is typically high CPU loads. When an attack is ongoing, users from the LAN side will no longer be able to send/receive traffic to/from the Internet. All firewalls we have seen recover when the attack stops.

We know that different firewall vendors have different implementations for handling this type of attack, but we also believe that especially vendors who state that ICMP should be allowed from outside are highly vulnerable to these kinds of attacks. We know that the RFC standards state that some ICMP types and codes have to be allowed, and also that if all ICMP is denied by default, something is likely to break down. We also know that having firewalls set to log all in a firewall will have a negative impact on the CPU during high traffic load.

What is ICMP Type 3 Code 3
Type 3 is Destination Unreachable
Code 3 is Port Unreachable

More information about ICMP Types and Codes can be found here:
http://www.nthelp.com/icmp.html

How to test if you are vulnerable

The best way to test if your systems are vulnerable, is to allow ICMP on the WAN side of you firewall and do some testing with Hping3. When attacking the WAN side of your firewall, try to do some internet surfing from the inside and out. In our test we used an Ubuntu installation with Hping3 installed. When testing, you have to be able to reach outbound internet speed of at least 15-18 Mbit/s.

Use Hping3 with one of the following commands:

Commands use with Hping3
hping3 -1 -C 3 -K 3 -i u20 <target ip>
hping3 -1 -C 3 -K 3 --flood <target ip>

Based on our test, we know that a reasonable sized laptop can produce approx. a 180 Mbit/s DoS attack with these commands. We have also made tests using a Nexus 6 mobile phone with Nethunter/Kali which only can produce 9.5 Mbit/s and therefore cannot single-handedly perform the BlackNurse attack.

When the test is running try to browse the internet from the LAN side of the firewall you are testing and keep an eye on the CPU load of your firewall. Firewall logging during the attack can increase the impact from the attack, which means that the firewall gets even more exhausted. We also believe that many firewalls with a single CPU is more likely to get exhausted faster than firewalls with 2 or more CPUs.

Detection

Based on our testing of BlackNurse, we have made a SNORT IDS/IPS rule to detect the attack.

In this rule it is important that 'count 250' and 'seconds 1' is adjusted to what is normal for your firewall. The default count and seconds as we have set them in the rule, should be fine for most firewalls. We recommend that event filters are used to prevent alert flooding in SNORT. This prevents that the IDS system becomes the victim.

More information about Event Filter.
https://www.snort.org/faq/readme-thresholding

SNORT IDS Rule to detect signs of the The BlackNurse Attack.

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"TDC-SOC – Possible BlackNurse attack from
external source "; itype:3; icode:3; detection_filter:track by_dst, count 250, seconds 1; reference:url,
soc.tdc.dk/blacknurse/blacknurse.pdf; metadata:TDC-SOC-CERT,18032016; priority:3; sid:88000012; rev:1;)

alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"TDC-SOC – Possible BlackNurse attack from
internal source"; itype:3; icode:3; detection_filter:track by_dst, count 250, seconds 1; reference:url,
soc.tdc.dk/blacknurse/blacknurse.pdf; metadata:TDC-SOC-CERT,18032016; priority:3; sid:88000013; rev:1;)
```

Impact

Based on our research, this vulnerability or misconfiguration of some firewalls is easy to misuse. Impact can be high for those that allow ICMP to the firewall's outside interface, and they could be easy targets for the BlackNurse attack as we have seen in TDC's network.

Having high bandwidth is no guarantee that this DoS/DDoS attack will not work. Many firewall implementations handle ICMP in different ways, and different vendors can be subject to attacks. Distributed attacks from larger botnets can be a major problem, because botnets which are located on low bandwidth uplinks can come into play.

We know that a small number (1 to many) of internet connections with uplink speed of around 15-18 Mbit/s can keep large companies or organisations under DoS/DDoS until they mitigate the attack.

Impact can be different from network to network based on what the network is covering. We recommend you test your own network.

Calculated Score based on CVSS 3.0
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:W/RC:R
Base score: 7,5
Temporal Score: 6,8

Common Vulnerability Scoring System Version 3.0 Calculator
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:W/RC:R

Mitigation

Different kinds of mitigations can be implemented to minimise the impact of the attack. On firewalls and other kinds of equipment a list of trusted sources for which ICMP is allowed could be configured. Disabling ICMP Type 3 Code 3 on the WAN interface can mitigate the attack quite easily. This is the best mitigation we know of so far.

The default recommendation from Cisco is the following:
We recommend that you grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP Path MTU discovery, which can halt IPsec and PPTP traffic.
See RFC 1195 and RFC 1435 for details about Path MTU Discovery.

More information about Cisco's default implementation
http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command/reference/cmd_ref/i1.html

We believe, that what we see when our customers get hit by the BlackNurse attack is that the firewall admins have just followed recommendations or misconfigured firewalls. Mitigation on firewalls could be to change default config or to patch any code that can lead to a DoS state.

Anti-DDoS mitigation
Use of professional anti-DDoS solutions from ISPs can mitigate the BlackNurse attack as well as other forms of DDoS attacks.

Special Thanks

Special thanks to all involved parties who have spent time testing for our team.

NETRESEC
Special thanks to Erik Hjelmvik from NETRESEC for helping with the analysis of packet dumps, testing on different systems and coming up with ideas for test scenarios.
http://www.netresec.com