The state of affairs regarding the recent DDoS attacks - September 2020

An insight into the recent DDoS attacks in 13 questions and answers

Is your question not mentioned here?
You can always contact the NBIP specialists via email. We are more than happy to answer your questions.

bureau@nbip.nl
nbip.nl/en/nawas

What happened recently?

Mitigating DDoS attacks via the NaWas is a daily task for NBIP, but the attacks that took place in August and September on the infrastructures of Internet Service Providers (ISPs) were of a completely different order. The DDoS attacks targeted routers and DNS infrastructures of the types DNS amplification, LDAP amplification and NTP amplification. The attacks were very intense, up to 260 Gbit per second. When an attack was stopped, the following attack started 30 minutes later.

What were the main characteristics of these attacks?

These attacks were extremely powerful (up to 260 Gbit per second) and sometimes lasted longer than four hours. They were targeted at ISPs in the Benelux. The attacks can be divided into four different categories: LDAP amplification (37%), DNS amplification (37%), NTP amplification (18%) and DNS request flood (10%).

What is LDAP amplification?

LDAP amplification exploits a specific weakness in older LDAP servers that are still in use - the CLDAP protocol. Originally intended to see what services are available on an internal network server, some servers have the UDP port 389 open to the "outside".

What is DNS amplification?

The attacker sends a DNS look-up request to vulnerable DNS servers with the spoofed IP address. Usually these are DNS servers that support

open recursive relay. The request is often passed on via a botnet so that the attack is bigger and better hidden. The DNS request is sent using the EDNS0 extension of the DNS protocol, which allows large DNS messages. The request can also abuse the cryptographic function of the DNS security extension (DNSSEC) to make the message larger.

What is DNS request flood?

This version of a UDP attack is one of the best known DDoS attacks. It specifically targets DNS servers to attack other web servers. It is also one of the most difficult attacks to detect and prevent. In order to carry out an attacker a large quantity of spoofed DNS request packets that look no different than real requests. These come from a very large number of IP addresses. This makes it impossible for the target server to distinguish between legitimate DNS requests and DNS requests that appear legitimate. The server gets overloaded trying to handle all requests - all bandwidth is consumed.

What is NTP amplification?

NTP amplification is a type of DDoS attack in which the attacker uses publicly accessible Network Time Protocol servers to bombard the target server with UDP traffic. NTP is one of the oldest network protocols and is used by connected devices to synchronize their clock. Older versions of NTP support a monitoring service that allows administrators to do a traffic count. This command is called monlist and it sends the requester a list of the last 600 hosts that have connected to the server. Since the sender is spoofed, the target of the attack will have to process an enormous amount of data.

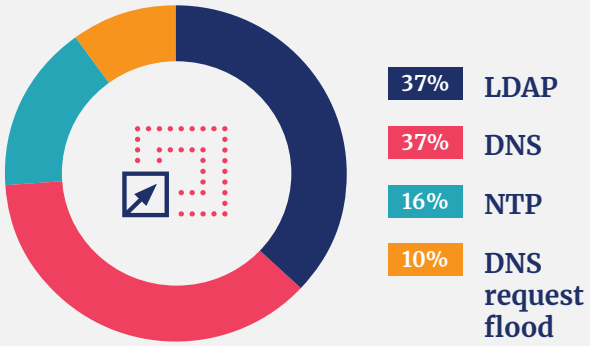
Which Internet service providers were affected?

The DDoS attacks were targeted, amongst others, at Caiway. On Tuesday the 1st of September, the provider suffered a major DDoS attack. On Tuesday afternoon, there was also a major attack on Signet. Signet also manages the infrastructure for TransIP and their customers also suffered disruptions as a result of that attack. The forum of the Belgian ISP EDPNet even talks about attacks up to 200 Gbit/s. This provider has had DDoS attacks for five consecutive days.

Were Internet Service Providers outside the Benelux affected as well?

Companies outside the Benelux were also attacked and had to deal with failure of Internet services.

Types of DDoS Attacks



NaWas was able to connect several new participants in a short period of time to combat DDoS and make the Internet more secure. Recently, NaWas expanded its presence to London at the London Internet Exchange (LINX), Italy with the connection of IT.Gate on Top-IX and the Vienna Internet Exchange (VIX).

Who is behind these DDoS attacks?

It is difficult to determine exactly who the attackers are. The profile of the attackers varies from script kiddies to countries that want to disrupt something with a DDoS attack.

What is the motive for a DDoS attack?

Attackers can have different motives. A DDoS attack may be intended to make an organization's website inaccessible, for example. In some cases, young people organize a DDoS attack purely out of enjoyment.

How to avoid a DDoS attack?

It is almost impossible for an individual company to avoid a DDoS attack. Avoiding a DDoS attack requires a solid infrastructure that costs a lot of money. By combining forces and expertise NBIP offers the NaWas to which internet service providers can connect. The NaWas is capable of separating 'right' and 'wrong' internet traffic. It sometimes happens that cyber criminals approach companies and say that they will stop a DDoS attack for a fee. NBIP always advises not to pay. Choosing NBIP's NaWas is a better solution. If your company is the victim of a DDoS attack, NBIP always advises to report it to the police. If organizations are members of the NaWas, NBIP makes a joint report on behalf of its participants.

What is NaWas?

The collective DDoS scrubbing center called 'NaWas' (loosely derived from the Dutch word for 'washing') has been operational since 2014 and automatically mitigates DDoS attacks for connected participants 24/7. By jointly procuring capacity, technology and knowledge and expertise, a highly effective mitigation of DDoS attacks is possible. The NaWas 'washes' the DDoS traffic clean and only sends clean traffic back to the NaWas participant. In this way, systems and services remain available and the DDoS attack is rendered harmless.

NaWas NBIP is a non-profit community driven Scrubbing Center from the Netherlands connected via AMS-IX, LINX and other major internet exchanges. NaWas is present at the Amsterdam Internet Exchange (AMS-IX), NL-IX and DCSpine and offers multiple ways to connect ISPs in Europe.

Who is the NBIP?

The Dutch National Internet Providers Management Organization (Nationale Beheersorganisatie Internet Providers, or NBIP for short) is a unique initiative of Internet providers that goes under the motto "Smarter and stronger together".
NBIP currently provides two services based on this collective idea: lawful interception, to execute wiretapping warrants, and the NaWas, an anti-DDos service. In the course of 2021, NBIP will introduce the Clean Networks service platform, which will allow ISPs to be informed actively and in real time about any vulnerabilities or exploits in their network. At the same time, NBIP will help these ISPs to solve these problems in their networks.

DDoS attack - number per Gbps (top 20)