Dear customer,

On Monday 22 March, TransIP was hit by a major DDoS attack targeting our entire infrastructure. As a result, your services and our websites were less accessible in the afternoon.

In this post-mortem we explain what happened during this attack, what measures we have taken at that time to mitigate its impact and what measures we are taking to prevent such an attack from having a major impact in the future.

**Background**

DDoS attacks and the components of the TransIP infrastructure involved in this attack are technical in nature. Knowledge of certain terms is necessary to be able to fully follow the events during the attack. We would therefore like to explain these terms below first.

**DDoS attack**

DDoS stands for Distributed Denial of Service and aims to make traffic to and from servers, computers, or networks impossible. Attackers use a network of infected and/or vulnerable third-party devices. These devices send an overwhelming amount of internet traffic to the target.

The result is that the attacked service (for example a website) starts to work very slowly, becomes partially or completely unreachable. In theory, a DDoS attack can be scaled up so that, regardless of the defensive party's network capacity, this goal is achieved.

There are several techniques that can be used for a DDoS attack. Last Monday's attack was so large that we saw every technique.

**DDoS scrubbing**

Scrubbing is a widely used technique to protect against DDoS attacks. Network traffic is cleaned in a process called 'scrubbing': DDoS traffic is stopped and only legitimate traffic is allowed to go through. A provider can perform this scrubbing process itself, or traffic can be redirected to a party that specializes in scrubbing. Such a party can usually handle much larger amounts of data traffic than the provider itself.

The advantage of scrubbing is that legitimate traffic passes through unhindered by the DDoS attack, unless the amount of network traffic from the attack is larger than the network of the scrubbing party can process.

A disadvantage of using an external party for scrubbing is that, due to technical reasons, a piece of legitimate network traffic is also stopped. Although very effective against large DDoS attacks, scrubbing through an external party is like shooting a mosquito with a gun. If the attack is not too large, it is therefore preferable to perform the scrubbing process at the level of the defending party: in that case legitimate traffic is not hindered.

**Blackholing**

Blackhole routing, or blackholing, is a technique that sends network traffic to a 'black hole'. All traffic to an IP address, good and bad, is routed to the black hole and 'dropped' there (all network traffic disappears).

The advantage is that the network load of the attack disappears. This also gives engineers the breathing space to make adjustments to further combat the attack. In addition, an attacker will also notice that his traffic disappears into a black hole. Major DDoS attacks are costly and usually setting up a black hole is reason enough for an attacker to stop attacking quickly. The disadvantage is that even legitimate traffic is temporarily stopped with this.

**DNS**

Domain names use DNS, which stands for Domain Name System. You can set up so-called DNS records for your domain name. DNS records tell systems, such as your Internet browser and email program, on which servers services such as the website and email of your domain name are hosted.

**Nameserver**

Your domain name's DNS records are stored on name servers. For example, as soon as you enter a domain name such as google.com in the address bar of your browser, a request is made to the name servers configured for the domain. The name servers then indicate, by looking at the DNS records, on which server the corresponding website is located. Name servers are a kind of telephone directory of the Internet.

**Packet loss**

Network traffic is divided into small pieces of data or ‘packets’. One or more packets not arriving at the destination, is referred to as packet loss. You experience this as a slow connection, or a complete or partial interruption of your connection.

**Timeline of the DDoS attack**

*13:30:* Our engineers receive a notification of a DDoS attack. It quickly becomes apparent that this attack is aimed at our nameservers, and that the attack is quite large. Our DDoS protection can clean the traffic through scrubbing so that the impact is minimal.

At the same time, we are notified that people who use the Internet through Ziggo are unable to access our website and domains that use our name servers. We immediately launch an investigation into the cause.

*14:00:* The volume of the attack decreases, but the problems of people using a Ziggo connection persist. In an effort to remedy this, we disable our automatic scrubbing. However, this does not solve the problems.

*14:30:* We find out that the problem with the Ziggo connections is caused by blackholing of the IP addresses of our name servers by one of our internet providers. This provider mainly processes traffic from Ziggo connections to TransIP. As a result, anyone using a Ziggo connection is unable to access our

website, and domains using our nameservers. Our engineers contact the relevant provider and the black hole of our name servers is quickly removed. We turn on automatic scrubbing again, because otherwise DDoS traffic will go unhindered.

A second, significantly heavier attack begins at the same time. This is a broader attack, not only targeting our nameservers but also other parts of our infrastructure. The amount of traffic during this attack is later than our network can handle. As a result, everyone who connects to our website and services hosted by TransIP is now experiencing packet loss issues.

*16:20:* Our engineers temporarily disable the internet traffic coming from some of our providers: a large part of the DDoS traffic appears to be mainly through the connections of a select few of our providers. By temporarily disabling these providers, we capture a very large portion of DDoS traffic. Legitimate traffic that passes through these providers is also temporarily stopped.

In addition, we blackhole several of our own IP addresses that are attacked but do not perform a crucial task at this time. The purpose of this is to show the attackers that their DDoS traffic is not going anywhere anymore. This is sufficient motivation to stop the attack in almost all DDoS attack scenarios and after a few minutes we see that this is also the case here: the DDoS attack decreases in intensity and our services become accessible again.

*17:45:* The situation has been stable for some time now. Our website and services hosted by TransIP are fully accessible again. We keep a close eye on the situation for the rest of the evening and night.

**Conclusions and measures**

First of all, we regret that you have been inconvenienced by this DDoS attack. The first attack was initially aimed at our nameservers and the second attack also targeted our internal infrastructure. However, the impact of these attacks was much larger: many of the domains using our nameservers were affected by this attack. The reason for this is twofold:

- During the first attack, our name servers were inaccessible to people with a Ziggo connection. This is because one of our providers has set up a black hole for the IP addresses of our name servers. This provider mainly processes Ziggo connections to our network. That its impact turned out to be so much larger is due to how DNS systems work:
  Domains use DNS records to indicate on which server(s) a domain is hosted, for example for that domain's website and email. An important part of DNS records is the so-called ‘TTL’, or the Time To Live. The TTL indicates how long it takes for DNS records to expire. After DNS records expire, they are retrieved again from the nameservers configured for that domain. If name servers become unreachable, as in this case by blackholing our IP addresses and during the second attack by the attack’s sheer volume, those DNS records cannot be retrieved. As a result, your computer does not know which server to connect to when you visit a website whose domain uses our nameservers for example.
- The second attack was so large that our own network could no longer handle the amount of traffic directed at it and there was significant packet loss. This could also interfere with the use of services hosted on TransIP servers, without those servers being the primary target of the attack.

Based on these conclusions, we take a number of measures to drastically reduce or even prevent the impact of a major DDoS attack in the future.

- We enter into a contract with a party that specializes in scrubbing. In DDoS attacks where our own network can no longer handle the amount of traffic, network traffic is redirected through and scrubbed by this party.
- The provider that set up a black hole for our nameservers has added the IP addresses of our nameservers to a whitelist, which will prevent this from happening again.
- Multiple physical and logical separations will be added to our nameserver setup. This makes our nameservers more resilient to DDoS attacks.
- We are investigating whether adjusting the TTL of both our domains and our customers, in cases where DNS management is automated through us, can limit the impact of these types of attacks. We will inform you by e-mail if this applies to your services and affects you.

Finally, we apologize for not being able to email you about this DDoS attack in a timely manner. Emailing all our customers takes a lot of time (longer than this attack took). This is why we use the page https://transnoc.nl which is separated from our own network. In the event of problems with our network, we can still inform you about its status. In addition, we will continue to use Twitter in such situations to inform you as soon as possible.

Should you have any further questions regarding this post mortem, do not hesitate to contact us via a message from your TransIP control panel.

Kind regards,

TransIP B.V.