NBIP NaWas

Protecting VoIP from DDoS attacks

Growing dependency on VoIP

The global market for VoIP services has grown exponentially over the past 20 years. It is now a $85 billion market and will continue to grow to over 100 billion over the next five years. Since the corona pandemic, more people have become dependent on VoIP. Think about all the online conversations and meetings with colleagues, business partners and customers. At the same time, people at home are also communicating more frequently with family members and friends via VoIP. That growing volume and increasing dependency presents VoIP providers with the challenge of improving the capacity and availability of their services and preventing outages.

DDoS attacks are a threat to VoIP

Like all other Internet services, VoIP is vulnerable to the increasing amount of DDoS attacks. In 2021, the number of registered attacks grew to 2860 in the Netherlands alone, compared to 1610 in 2020. They also grew in size to 319 Gbps versus 200 Gbps in 2020 and 124 Gbps in 2019, while lasting longer than 4 hours on average. When those DDoS attacks disrupt VoIP services, or inconveniently slow them down, it leads to both immediate revenue loss and longer-term reputational damage. Currently, VoIP traffic is attacked less than other data traffic, but the business impact of a VoIP disruption is always significant.

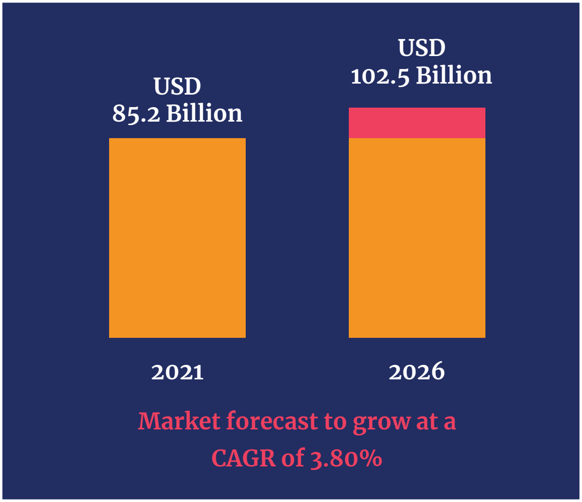
Number of attacks: **700**

Average number of attacks per day: **7,6**

Maximum size of attacks **308Gbps**

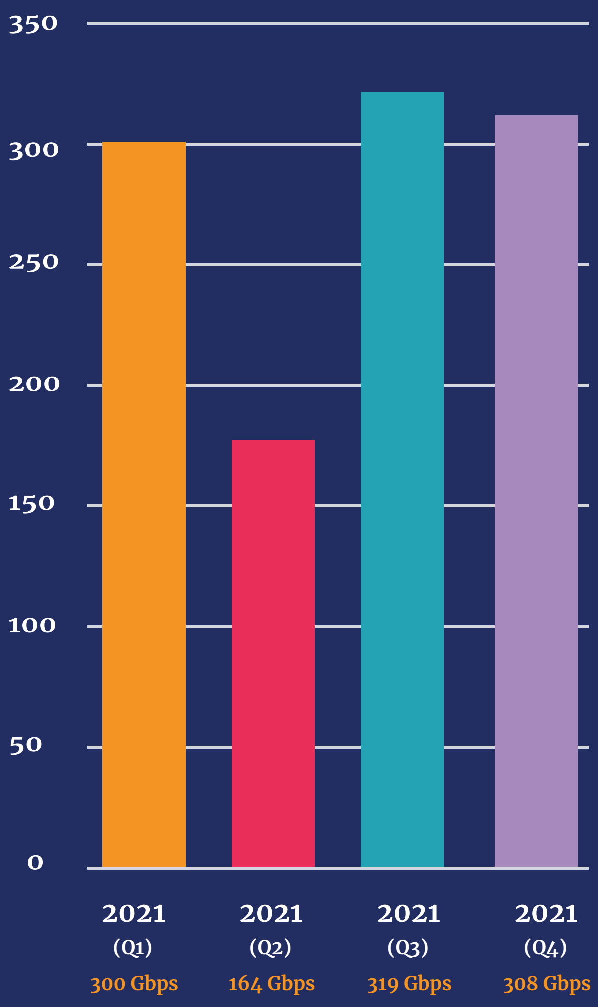
source: NBIP - Infographic - DDoS data - 2021 Q4 - NL.pdf

Global VolP Services Market



Market forecast to grow at a CAGR of 3.80%

Maximum size of attacks



DDoS attack on UK infrastructure

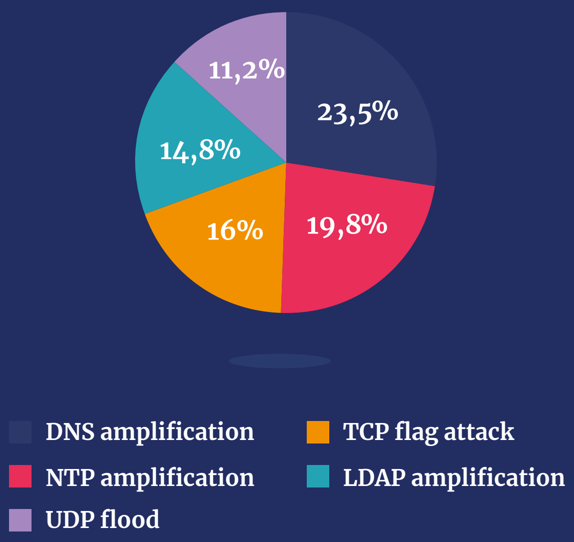
The DDoS attack on UK communications infrastructure in the fall of 2021 was a pervasive wake-up call. Telecom executives have spent night and day, to fix it and to ensure they are better prepared next time. During discussions between the Comms Council UK and the CCA, it was decided to work more closely with the UK government, the National Cyber Security Centre, Ofcom and international agencies, to stop this kind of criminal activity as soon as possible. All organizations agreed that strategies and solutions need to be developed in order to limit further damage.

VoIP-trends

The use of VoIP is rapidly growing because of its flexible and scalable capacity and its ease of integration with other IP communications applications. In the coming years, the popularity of VoIP will be further propelled by the increasing number of fiber optic connections and the adoption of 5G, which will ensure both higher speeds and better quality. But also due to new AI applications for customer service, VoIP support for the rapidly growing number of IoT devices (such as cameras), and the retirement of analog phone systems. This is a bright outlook for all VoIP providers, with the downside of increasing security risk. In addition to the business-critical VoIP traffic, the underlying databases are particularly valuable targets.

Protecting VoIP

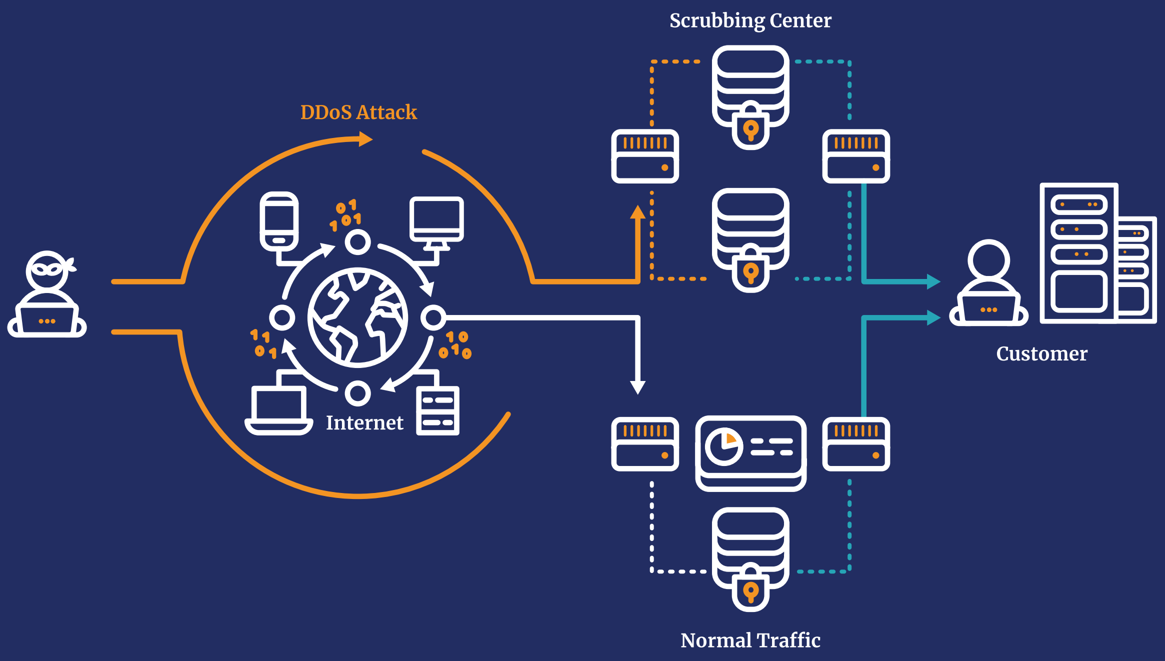
VoIP has more UDP traffic than TCP and uses RTP for the audio and SIP for the necessary handshaking. Of course, ISPs and VoIP providers handle all of these protocols because they are part of the overall IP traffic. VoIP traffic differs from other IP traffic in some important ways because it is time-critical (latency) and real-time. There should be no delays during calls, so VoIP is quickly disrupted in a DDoS attack. Mitigation of an attack must take this into account. Another aspect that comes into play during a disruption of VoIP traffic, such as in a DDoS attack, is that calls to emergency services can also be disrupted. This is an additional reason to protect VoIP as best as possible. NaWas can help with this.



source: NBIP - Infographic - DDoS data - 2021 Q4 - NL.pdf

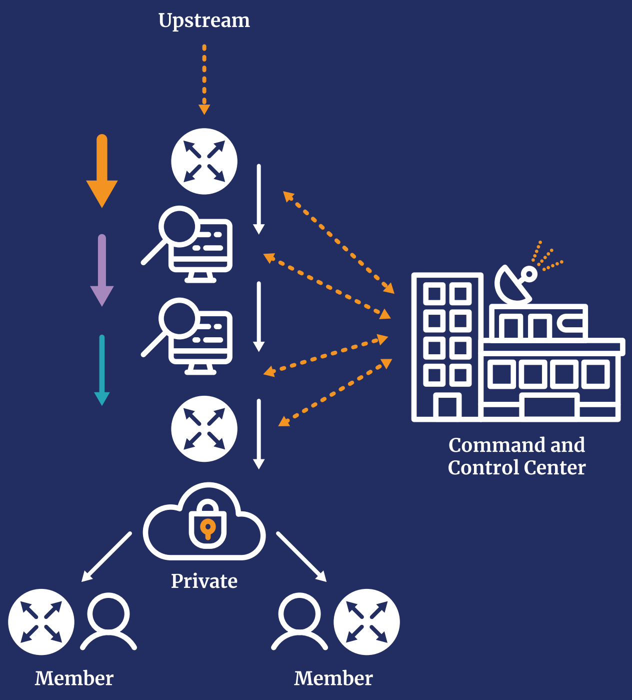
Joining forces to counter DDoS attacks

Like ISPs, VoIP providers must ensure quality, availability of service and protect customer information. This can be done by individually investing in and maintaining effective security solutions, or by joining forces through NaWas. NaWas is part of the non-profit organization NBIP, in which more than 200 ISPs have joined forces since 2002 to protect against cyber attacks. A key service we provide is the DDoS Scrubbing Center NaWas, which protects over 6.5 million domains and 1.5 million websites with state-of-the-art cloud-based security solutions. This service is available in many countries in Europe and the UK.



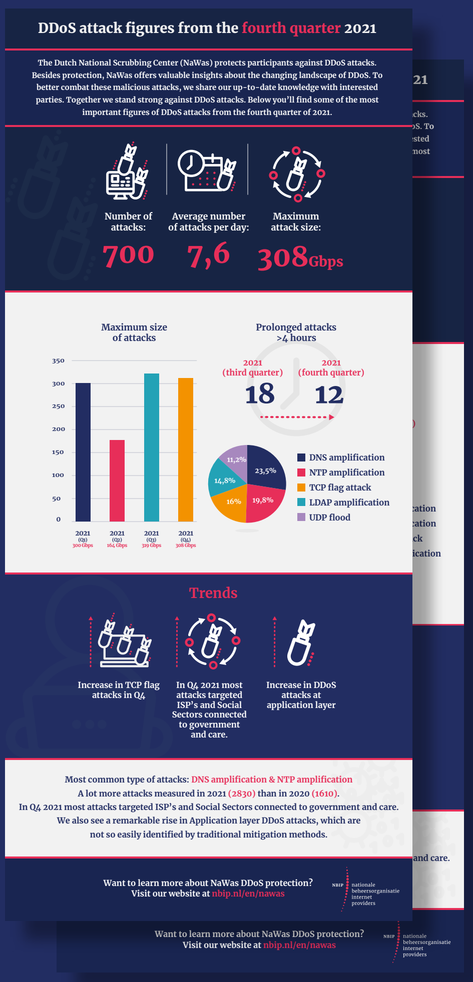
How does NaWas work?

NaWas protects VoIP providers by quickly detecting a DDoS attack, washing all suspicious traffic through our mitigation street and then returning the clean IP traffic through one of the connected Internet Exchanges. To do this, we use several tier 1 Internet transits and public peering on Internet Exchanges, a DDoS Scrubbing Center and failover sites created with security solutions from different vendors and private connections to AMS-IX, NL-IX, Dcspine, Linx, MIX, Top-IX, Namex and Netix. Furthermore, NaWas uses baselines for customer-side detection and several mitigation methods during redirection and cleanup to effectively protect VoIP traffic without too much latency. As more and more ISPs and VoIP providers join NaWas, the synergy is also increasing.



R&D and reporting

As a non-profit organization for ISPs and VoIP providers, NBIP and NaWas also invest in techniques for legally compliant interception and analysis of IP traffic. But also against the distribution of unlawful content through the Clean Networks Platform. The results of our investments, R&D and collaborative initiatives are regularly reported and shared with all member ISPs and VoIP providers, so that together they can benefit from the lessons learned and best practices. An example is the quarterly update we release on all recorded DDoS attacks.



DDoS attack figures from the fourth quarter 2021

The Dutch National Scrubbing Center (NaWas) protects participants against DDoS attacks. Besides protection, NaWas offers valuable insights about the changing landscape of DDoS. To better combat these malicious attacks, we share our up-to-date knowledge with interested parties. Together we stand strong against DDoS attacks. Below you'll find some of the most important figures of DDoS attacks from the fourth quarter of 2021.

Number of attacks: 700

Average number of attacks per day: 7,6

Maximum attack size: 308Gbps

Trends

Increase in TCP flag attacks in Q4

In Q4 2021 most attacks targeted ISP's and Social Sectors connected to government and care.

Increase in DDoS attacks at application layer

Most common type of attacks: DNS amplification & NTP amplification
A lot more attacks measured in 2021 (2830) than in 2020 (1610).
In Q4 2021 most attacks targeted ISP's and Social Sectors connected to government and care.
We also see a remarkable rise in Application layer DDoS attacks, which are not so easily identified by traditional mitigation methods.

Want to learn more about NaWas DDoS protection?
Visit our website at nbip.nl/en/nawas

NBIP nationale beheersorganisatie internet providers

Want to learn more about NaWas DDoS protection?
Visit our website at nbip.nl/en/nawas

NBIP nationale beheersorganisatie internet providers

European collaboration

More and more ISPs, VoIP providers, suppliers and governments are realizing that international cooperation is essential to effectively stop DDoS attacks. Therefore, NaWas is working closely with a number of European Internet exchanges, such as Linx in the UK and MIX & Netix in Italy. Thanks to our market development in other European countries, the number of NaWas partners continues to grow. Finally, we also work together with the Dutch Anti-DDoS Coalition, in order to allow the business community, governments and universities to benefit more from all the available knowledge and experiences.

NaWas benefits for VoIP providers

Like all connected Internet Service Providers, any VoIP provider can benefit through NaWas:

- Proven effective protection against DDoS attacks;
- Reduce risks of VoIP disruption and delay;
- Lower CAPEX and OPEX for DDoS protection;
- Shared knowledge and experience;
- 24/7 support including a NOC;
- Redundant setup for multi-vendor mitigation;
- Support in setting up and running detection, or Detection-as-a-Service (Daas)

Testimonial from VoIP providers

As a VoIP provider, Speakup has been a regular target of DDoS attacks," says Rick Sulman, CEO of Speakup. "With NaWas from NBIP, we have an effective solution to mitigate these attacks. Tuning the service to specific VoIP requirements was taken up with NaWas and is now working very well. Thanks to the cooperation between Speakup and NaWas, both parties have gained a lot of knowledge about mitigating DDoS attacks on VoIP services. We did not have any significant service interruptions since working with NaWas. We are very satisfied!"

> *"With NaWas, we have an effective solution to mitigate DDoS attacks. Tuning the service to specific VoIP requirements was handled together with NaWas and is now working very well."*
>
> *– Rick Sulman*
> *CEO of Speakup*