CASE STUDY

GARR CHOOSES CORERO FOR AUTOMATED DDoS PROTECTION

GARR is the ultra-broadband network dedicated to the Italian research and education community. Its main objective is to provide high-performance connectivity and to develop innovative services for the daily activities of Italian researchers, professors, and students, as well as international research collaborators.

The GARR network is an extensive digital infrastructure with about 15,000 km of optical fiber covering the entire Italian territory. It reaches about 4 million users of about 500 organizations and connects more than 1,200 sites, most of which are public institutions (research institutes, universities, research hospitals, cultural institutes, libraries, museums, schools). The GARR network is interconnected with international research networks and across the worldwide Internet.

The GARR governance model promotes inclusiveness and involves users in decision-making on the future evolution of the network and digital infrastructures. Unlike with commercial providers, users on the GARR network aren't just consumers of data, content and services; they are involved in the development of services and solutions, and they share their own resources for the benefit of the scientific community, thus becoming active contributors.

> Corero Smartwall at a glance

- Surgically removes DDoS attack traffic automatically, before it reaches critical systems, ensuring optimal performance and maximum availability.
- Delivers line-rate, in-line distributed denial of service attack protection, from 1Gbps to 100Gbps per rack unit, in a solution that scales to Terabits per second of protected throughput.
- Prevents the impact of attacks ranging from simple volumetric floods, to sophisticated state exhaustion attacks, at layers 3 to 7.
- Delivers comprehensive visibility for analysis and forensics, before, during and after attacks.

>the challenge

Over the past 10 years, GARR has been targeted by DDoS attacks; during the same period GARR has worked proactively to ensure its network nodes are not the source of any such attacks against other organizations.

This was accentuated with the connection of schools to the network, starting in 2012; where, today, more than 1,000 schools are now directly or indirectly connected to the network. The turning point came in 2016 when the impact of long-term, volumetric DDoS attacks compromised primary network functionality, effectively preventing access to Internet services. This led GARR to adopt extreme solutions such as RTBH (Remotely Triggered Black Hole Filtering), a brute-force mechanism that unfortunately blocks both good and bad traffic for the victim target but does allow connectivity service for the rest of the services on the network.

More recently, GARR observed an evolution of the DDoS attacks they are being targeted with; they became shorter in duration and more widely distributed on the network. They often received several DDoS attacks each day (<50 per month), each of which lasted less than 30 minutes. Most of them were large enough to impact the user experience on the network, and a few were severe in terms of upstream saturation. This new class of DDoS attacks made it impossible for GARR to react quickly enough and led to the decision to look for a more effective detection and mitigation mechanism.

GARR is also known as the Italian Research and Education Network, supporting projects involving scientific and academic cooperation among Universities, Schools, and Public Research Institutions in Italy. Like other national research and education networks, GARR has a combination of research-related traffic, and general Internet traffic. Each *"user institution"* has its own network, which typically has thousands, or even hundreds of thousands, of individual users. With its more than three million IPv4 public nodes and its pioneering infrastructure that dates back to the early 1990s, the GARR network has always worked to minimize any attacks that were sourced from one of the nodes in their network.

In 2019 GARR carefully researched the available DDoS mitigation solutions, and finally selected Corero's SmartWall® Threat Defense Director solution, because it seamlessly integrates with their existing procedures and organizational structure, and because it works synergistically with GARR's existing Juniper Network infrastructure. The SmartWall Threat Defense Director couples Corero's surgically accurate, real-time, automatic DDoS protection with the high-performance packet filtering of GARR's Juniper MX Series routers.

> **"In contrast to other mitigation solutions, based on scrubbing center technology, that would have to reroute attack traffic to a single very expensive device, Corero TDD blocks attacks directly on the Juniper MX nodes we have at all our PoPs, enabling us to block them in a distributed and simple way" said Massimo Carboni, CTO - Head of Infrastructure Department at GARR.**

This architecture also allows GARR to simply increase the scale of the protection in lockstep with any future network extensions.

Another key factor in GARR's decision was that Corero TDD is more suited to the very high throughput of the GARR network, where other solutions would introduce significant risk of misinterpreting traffic bursts as attacks, resulting in disruptive false positives.

Results for GARR

- No need to blackhole or null route all traffic to a DDoS target
- Negligible false positives impacting legitimate traffic
- Maximum levels of service availability are maintained for users, even in the face of a DDoS event
- DDoS attacks are automatically mitigated locally at each of their PoPs, avoiding the need to backhaul traffic across the network for mitigation
- Increased staff efficiency resulting from the automatic and accurate protection
- Increased user satisfaction resulting from the speed and accuracy of protection

>the benefits

> *GARR values the automated, hands-off efficiency of the Corero solution, which frees up staff to work on other tasks; "Thanks to the Corero solution, we operate more efficiently, so we estimate that we're saving about 20% in terms of staff time dedicated to network security," said Carboni. "It's clear that no human, or even a team of 10 security analysts, could react quickly enough to manage these sophisticated DDoS attacks," said Carboni. " For some types of attacks the solution is so fast that we had to review our Acceptable Use Policy and the security incident workflow, because in most attacks no human intervention is needed to tackle the problem."*

The Corero solution also delivers comprehensive visibility into attacks with the SecureWatch® Analytics component of its TDD solution, which leverages Splunk software for big data analytics and visualization capabilities that transform security event data into sophisticated dashboards. This information engine enables GARR to create custom dashboards and foster its own statistic and report systems integration *"We definitely like having visibility into attacks, knowing not only when and how an attack is happening, but also the ability to follow the mitigation process,"* said Carboni. *"This provides a higher level of control in security and increases our trust in the solution."*

GARR reports that Corero greatly improved the organization's end-user experience. GARR users are an active part of the research network and, in the past, they were often unaware of any DDoS attacks, so they considered any downtime or lack of service as a network problem. The DDoS mitigation service is a benefit to all the users. For the future, GARR is considering integrating its Corero SmartWall Analytics with its customer-facing portal, to better communicate with their users about the DDoS attacks they are being targeted with.