

Case History

PromiGroup

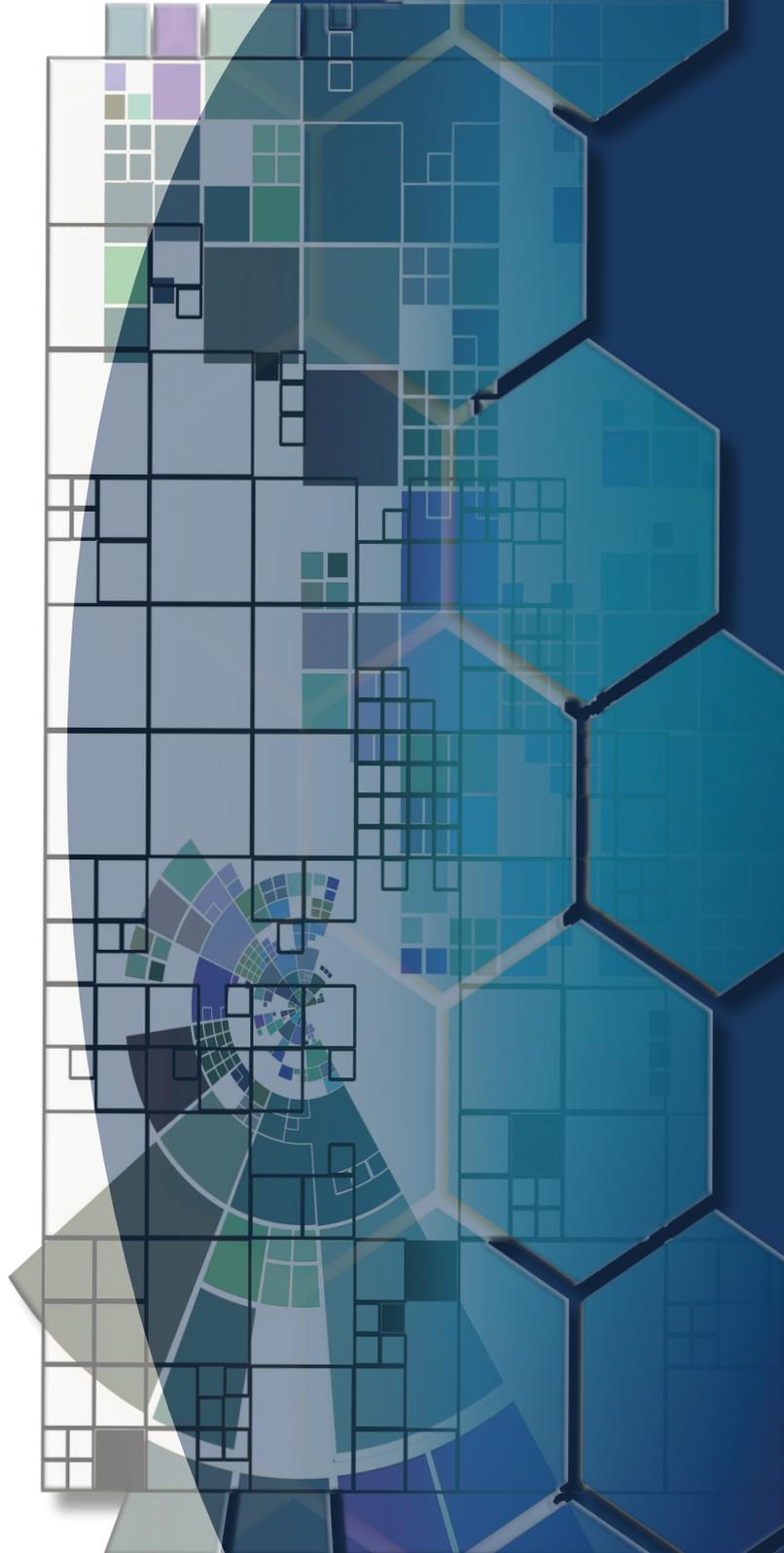
Ransomware attack: timely resolution



A well-known Italian company

operating in the integrated water service in 137 municipalities in Novara and VCO (Verbano-Cusio-Ossola), has chosen **PromiGroup** for a disaster recovery after a Criptoloker virus attack.

Last December, in fact, the customer, who had already implemented and renovated his IT structure with our team of certified technicians, **suffered a hacker attack**, called Riuk, launched in order to obtain a ransom of over **€200,000 in bitcoin**





The opening of an infected email, seemingly harmless, by a user of the company, **allowed the spread of the ransomware**, which quickly spread over the entire IT infrastructure, causing the **encryption of the network and the data**.

The repercussions of that? **The forced closure of the company for 48 hours**, the total blocking of some public services to end users, as well as a significant **loss of turnover**.

PromiGroup

The main causes

Among the main causes of the vulnerability of the systems, found by our team, there are:

- Safety Solution Endpoint Protection inadequate.
- Solution Behavioral Safety Software ineffective.
- Lack of internal user information on security.

The Intervention

The intervention of PromiGroup, by our team of certified technicians, **has allowed** not only **to deal with the cyberattack in a timely manner**, but also **to replicate live the actions of the hackers** who continued to act to counter our actions.

The perpetuated actions involved:

- The isolation** of the entire ICT infrastructure and Internet connectivity.
- The total ripper of the pre-attaque data**, thanks to the use of Dell Data Domain & veeam.
- Distribution of the entire ICT and PDL infrastructure of the **Sophos Intercept X solution with EDR.**

A constant support



Thanks to our expertise and with the help of DELL-VEEAM and SOPHOS solutions, it has been possible to make the entire ICT infrastructure operational again, and consequently all remote users and locations, in just two days.

Throughout the following week, PromiGroup provided ongoing support, both on-site and remotely, to consolidate the company's security.

PromiGroup

PromiGroup



Eletto Miglior Partner italiano
2016
Dell Emc