EDERSA SUCCESS CASE

UTILITY COMPANY DECISIVELY TACKLES “MINOR THREATS” THAT WERE PAVING THE ROAD TO RANSOMWARE.

EMPRESA de ENERGIA RIO NEGRO S.A.

EDERSA holds a critical role in the regional energy industry of Río Negro in Argentina. With more than 400 employees and 20 years of experience, they are responsible to over 220,000 clients for the public distribution, commercialization, generation, and supply of electricity.

SUMMARY

Electricity is the lifeblood of any community or enterprise, so the companies in this industry must ensure that they operate continuously without interruptions. This case study shows how Lumu helps to operate Edersa on a day-to-day basis.

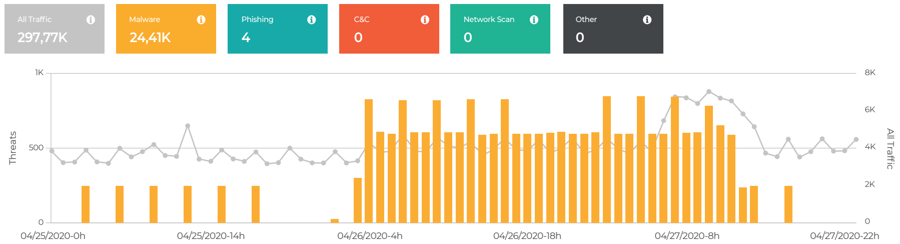
THE PROBLEM

Edersa realized that a modern cybersecurity strategy pays attention to all signs of compromise, no matter how insignificant they may seem. Therefore, they set out at the beginning of 2020 to illuminate the blind spots used by threat actors that can lead to unwanted situations:

- **Lack of compromise visibility:** Their network was showing inexplicable increases in resource consumption. This began to raise the suspicion that the network was probably compromised.
- **Difficult-to-pinpoint compromised assets:** They had no easy-to-operate tool that would verify if the network was really compromised. Additionally, if it was, it was necessary to quickly and precisely identify which devices were compromised.
- **Increase in alert generation:** Some perimeter security tools were showing an increase in the number of incident alerts, which also resulted in fatigue for cybersecurity operators due to the need to constantly modify rules and exceptions in said tools.
- **Ignored spambox and phishing attacks:** Phishing attacks are usually filtered by the organization's spam filter. However, this causes a loss of visibility into the content of that phishing and how it is trying to attack an organization's employees.

THE SOLUTION

Thanks to deploying Lumu easily and free of charge, Edersa was able to identify and understand the compromise within its corporate network in a couple of days. With Lumu they were able to analyze more than 300,000 queries and more than 24,000 threat contacts, allowing them to understand the nature of the compromise and thus determine how, when, and where criminals had compromised their network.



Lumu detected phishing attacks against Edersa employees in which user credentials could have been involved. Additionally, Lumu revealed malware creating thousands of domains and IP addresses generated through domain-generated algorithms (DGA), which are used by criminals to send and receive malware instructions to other compromised networks (usually called "command and control" or C2).

THE RESULTS / HOW LUMU HELPED

Edersa’s team could identify and isolate compromised computer equipment andreduced the time needed to respond to incidents since it allowed them to automate tasks.

Lumu reduced the amount of alert noise, relieving the burden and pressure on cybersecurity operators.

Lumu reduced the risk of reputation loss since the Conficker malware could have exposed Edersa as a generator of attacks on other companies.

Edersa saw evidence that their employees were at risk of having their corporate access credentials stolen in targeted phishing attacks that were not within the visibility of the cybersecurity teams.

> “Lumu gave us extensive threat visibility and real-time notification of ongoing incidents”.

CONTACT LUMU
SALES@LUMU.IO

www.lumu.io

ILLUMINATING THREATS AND ADVERSARIES