CASE STUDY

UTILITY COMPANY PROACTIVELY ENSURES UNINTERRUPTED SERVICE

This public utility company sustainably and efficiently supplies potable water to the population of one of the world's megacities, while providing ancillary services and acting as custodian to its surrounding environment. To accomplish that mission they oversee the activities of thousands of employees responsible for meeting the needs of approximately 15 million households.

SUMMARY

Considering the importance of the essential services they provide, this organization does not neglect its security. Even though this public services company already has mature cyber defenses in place, they recognize the importance of continual improvement. Lumu helps them evaluate and improve the effectiveness of their cyberdefense as a whole, as well as to detect compromises at speed, thereby ensuring the continued delivery of services to the people of one of the world's most populous cities.

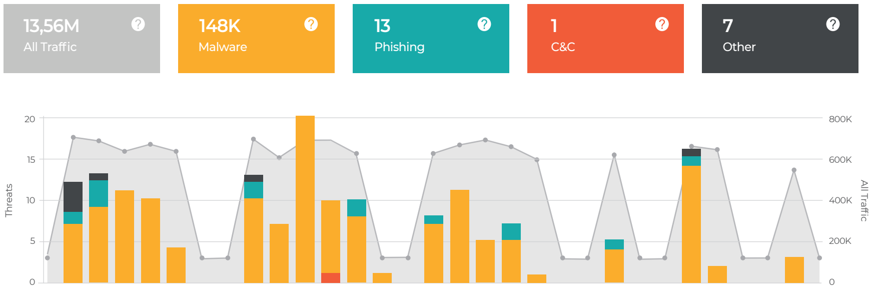
THE PROBLEM

As a critical infrastructure provider of national strategic importance, they need to assure that their service runs uninterrupted. With more and more connected devices for their legions of employees and a complex and distributed infrastructure model, they want to go above and beyond regarding the best cybersecurity practices. This company wanted to proactively address the following factors:

- **Cybersecurity benchmark:** It is critical for this public service provider to know their level of compromise to help them understand how resilient they were to cyberattacks.
- **Efficiency of their cybersecurity technology stack:** As a company with an advanced cybersecurity program, they need to optimize their existing cybersecurity tools and ensure they are delivering the expected level of protection.
- **Unified compromise visibility:** With information assets on-premise and beyond the perimeter, they want visibility into more than 8,000 assets to have a unified view of any compromise that could potentially affect the organization.
- **Support their business continuity plan:** Keeping in mind the importance of the service that they provide, they need to have maximum visibility into potential compromises. With this visibility, they can quickly activate containment and remediation plans, and prevent any kind of operational interruption.
- **IT/OT Integration:** Their extensive Operational Technology (OT) network controls thousands of physical devices to ensure that public services are delivered. Any attack could impact millions of people. Being proactive in detecting, mitigating, and eliminating the attacks is essential.

THE SOLUTION

With a smooth and easy deployment, Lumu was able to measure compromise across thousands of assets. In the first month, more than 13 million records were analyzed resulting in more than 100 compromises detected such as trojans, droppers, and crypto mining threats.



13,56M All Traffic

148K Malware

13 Phishing

1 C&C

7 Other

Having this unique view, the public service company is able to know early and exactly where the compromises are taking place, and take immediate and proper action to mitigate and eliminate before any harm is caused to the organization. That was possible because Lumu detects compromises in every stage of the cyber kill chain, allowing them to take proactive action.

THE RESULTS:

Real-time compromise benchmark: With Lumu, the public service company is able to know their exact level of compromise at any time and understand where and how to adjust their cybersecurity strategy to avoid breaches and their operations being affected.

Cybersecurity stack efficiency: With important cybersecurity investments, they now know with certainty when a tool needs to be optimized in order to unlock all its value. Lumu is also helping them identify gaps in protection, informing future cyberdefense investments.

Complete compromise visibility: With distributed customer service representatives to have full compromise, visibility is a must. With Lumu they are able to see a compromise in those devices without installing agents.

Support their Business Continuity Plan (BCP): They now have the needed information about ongoing compromises to activate their BCP at an early stage, before threat actors can affect the important service they provide.

> The only thing our cybersecurity stack was missing was the ability to monitor itself. Lumu fills that gap by providing us with baseline information to build upon and has become the keystone that makes our entire security posture more resilient.

CONTACT LUMU
SALES@LUMU.IO

www.lumu.io