CASE STUDY

FINANCIAL INSTITUTION ENJOYS UNPRECEDENTED COMPROMISE VISIBILITY

This financial institution has a presence across North and Latin America, where it sells over 3 billion USD of various financial services to corporate clients in various market segments as well as individuals. To their customers, the value of the assets protected exceeds their face value. This financial institution has never fallen victim to any major breaches—and seeks to maintain that record.

SUMMARY

This leading financial institution is now able to better protect its most valuable assets—its reputation, its clients, and their financial security. By incorporating Lumu into its security strategy they are able to gain real-time detection of compromises, a better understanding of its level of compromise, and insight into the effectiveness of its security strategy.

THE PROBLEM: VALIDATE THE EFFECTIVENESS OF THEIR CYBERSECURITY STRATEGY

In its industry, the stakes are higher than most. With tens of billions of dollars in assets, such institutions are huge targets for cybercriminals. According to the 2019 ITRC End-of-Year Data Breach Report, the financial sector accounted for over 60% of sensitive records exposed by breaches in 2019. In addition, a single public breach would erode the trust that their clients and stakeholders place in them. Recognizing these threats, they place a high value on their security.

The first challenge is to be able to detect any compromises at speed. Not just content with relying on their defenses, such a financial institution wants to know that if a threat actor succeeds in compromising a device from the organization, it will be detected immediately and its team will respond accordingly before any damage can be done.

With several locations, a complex hybrid environment, and thousands of distributed employees and contractors—as is typical for their industry—their security strategy needs to find a balance between protection and detection. It is an ongoing challenge to know where additional security protection is needed, where existing solutions are underperforming, and where additional investment is required. As a result, such institutions need to gauge the effectiveness of their cybersecurity strategy.

> "For us, **Lumu** has given us unprecedented compromise visibility. At an operational level, we use the intelligence provided to prioritize and respond to alerts. At a strategic level, we use this factual data to understand our posture and make the necessary changes to optimize our current stack and inform future investments."

HOW LUMU HELPED

Their security team is able to spend their time on what really matters. In the first months, Lumu detected nearly 200 compromises in the first 6 months.

The financial institution was able to identify that more than three-quarters of these compromises were malware. With that information, they adjusted their cyberdefense according to that challenge.

Their security testing methodology became fortified with Continuous Compromise Assessment, which allows them to know the type of compromises and where they are located in real time with factual data. This fortification extends to the whole organization's assets, not only their critical ones.

They are able to determine the effectiveness of their security stack with information to make better decisions and by having a continuous baseline to compare against.

CONTACT LUMU
SALES@LUMU.IO

www.lumu.io

LUMU ILLUMINATING THREATS AND ADVERSARIES