CASE STUDY

FINANCIAL INSTITUTION REDUCES RANSOMWARE DWELL TIME

This institution has more than 60 years' experience in banking and financial services and has grown to employ more than 10,000 employees spread across flourishing branches in several countries. Because of the global increase in ransomware attacks targeting important financial institutions, they were looking for a solution that can improve their cybersecurity posture and resilience.

SUMMARY

This world-class financial institution now enjoys the peace of mind that comes with continuously and intentionally measuring their state of compromise. They have seen first hand that when ransomware is detected they have the factual information to swiftly and effectively stop the attack in its tracks. They can also take comfort in that even when no compromises are showing up, Lumu's Continuous Compromise Assessment is still monitoring their network metadata in real time.

THE PROBLEM: DETECT RANSOMWARE AT SPEED

Ransomware is on the rise, and this financial institution realized they faced a growing problem: they could not say with certainty if an attack was already underway. Their strategy was two-fold. If they were under attack, they needed the ability to contain it quickly and minimize its impact. If they were not exposed, they wanted to know that their network was being actively monitored.

Global statistics show that this threat is getting worse:

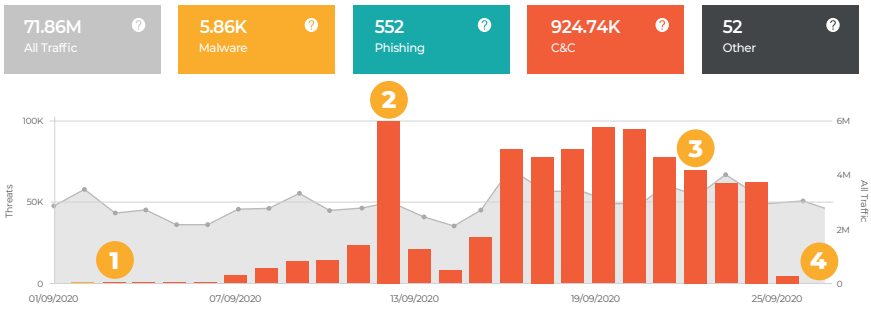
- The global cost of ransomware increased from USD 11.5 billion in 2019 to USD20 billion in 2020.
- Every 11 seconds a business will be attacked by ransomware in 2021.
- 36% of victims paid the ransom.
- 17% of the victims that paid a ransom never recovered their data.

With multiple financial institutions being a big target for ransomware attacks, to detect the attacks in minutes vs. months is a must. This financial institution knows that thousands of their assets could be the entry points for a devastating attack. Their strategy is to go beyond the traditional security testing practices required by law and try a new approach.

THE SOLUTION: IMPLEMENT CONTINUOUS COMPROMISE ASSESSMENT

Knowing they were sitting on a gold mine with their network metadata they decided to start the implementation of Lumu. Lumu was able to process millions of queries without the need to make any hardware investment as it is a cloud-based solution and detect compromises in the first minutes.

With that proof of value and with the detection of Maze ransomware they were determined to stop this threat before any real harm is done. Maze is one of the most destructive ransomware groups and to have this information is the difference between stopping the attack or being the next headline.



1. **Lumu** starts detecting contacts with Maze ransomware infrastructure in the first minutes reducing the dwell time
2. Upon communication blocking, the ransomware becomes more aggressive and begins moving laterally
3. Clean up process swiftly begins thanks to the intelligence derived from **Lumu**
4. The Maze ransomware related compromise is eradicated

HOW LUMU HELPED

Lumu started detecting contacts with Maze ransomware. Maze is not only a malware family, it is a complete business operation that integrates multiple parties. Detecting and stopping this threat as soon as possible is the difference between suffering immense financial and reputational losses, or carrying on with business as usual.

Knowing this information, they started the mitigation phase by blocking connections between the ransomware and adversarial infrastructure. After that, the ransomware became even more aggressive and began to move laterally. For that reason, it is important not only to mitigate, but to eradicate the compromise.

With all the information and context provided by Lumu they swiftly began the eradication process on all the affected information assets. The process was easy because they knew exactly where the compromises were and how to respond.

After the eradication process Maze ransomware was eliminated. They now have peace of mind knowing that no new contacts have been made, and they now have the information they need any time they face a similar situation in the future.

"Knowledge is power, and with Lumu we can know exactly which devices are infected by ransomware. The problem with this threat is that you usually only notice the problem when it is already too late, but with **Lumu** we reduced the dwell time of detection from months to minutes with a simple and straightforward installation."

CONTACT LUMU
SALES@LUMU.IO

www.lumu.io