CASE STUDY

HEALTHCARE PROVIDER STRENGTHENS BUSINESS CONTINUITY WITH LUMU

A healthcare institution with more than 10,000 information assets, 60,000 associated healthcare professionals, and 950,000 patients must protect the personal health information (PHI) of the people who entrust their health and privacy to them and ensure the continuity of their medical service. This institution has never been breached but knows that healthcare is a highly targeted industry and wants to be at the forefront of compromise detection.

SUMMARY

For any healthcare institution, patients are an absolute priority. With Lumu this institution can protect their patients' and employees' confidential information. Now they have peace of mind knowing that they can determine if they are compromised with one click.

THE PROBLEM: MEASURE AND UNDERSTAND COMPROMISE

In May 2020 the United States Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), and the United Kingdom's National Cyber Security Centre (NCSC) issued a joint alert of APT groups targeting healthcare and essential services in order to collect bulk personal information, intellectual property, and intelligence. The healthcare information is extremely valuable and the stats show that the problem is getting worse in this industry:

- Between 2009 and 2019 there were 3,054 healthcare data breaches that involved more than 500 breaches each.
- The number of exposed records more than doubled between 2017 and 2018, and more than tripled between 2018 and 2019.
- In 2019, healthcare data breaches were reported at a rate of 1.4 per day.
- A woman seeking emergency treatment for a life-threatening condition died at the Duesseldorf University Clinic in Germany due to a Ransomware attack.
- In 2020 several breaches in healthcare were reported, including Health Share of Oregon, Florida Orthopaedic Institute, Elite Emergency Physicians, Magellan Health, BJC Health System, and many more.

When an industry is a high-value target for cybercriminals, preparedness is key. They are going to relentlessly work to achieve their objective, so having the proper tools to detect attacks is key.

The first challenge for this healthcare institution is to be sure that they are not already compromised. Honoring the trust of their patients is everything and they do not want to add to the statistics of healthcare institutions that have failed to protect the confidential data of their patients.

THE SOLUTION: IMPLEMENT CONTINUOUS COMPROMISE ASSESSMENT

Unable to conclusively answer if the adversary is already inside, they decided to try Lumu in order to answer that question. They were impressed by the easy implementation process and they used the Lumu Free account to start their compromise assessment journey.

After a few minutes of implementation, they were able to see contacts of their information assets to malware and phishing sites. With the compromise context offered by Lumu they were able to identify, contain, and eradicate the compromises. They now have a baseline for their state of compromise and they can easily answer both if they have been compromised and where action is required.

With this proof of value, they were determined to develop the maximum available visibility, so they upgraded to Lumu Insights. This upgrade analyzes more metadata sources, gives greater visibility, and lets them know exactly where the compromises are.

HOW LUMU HELPED

In the first month of operation and after analyzing more than 7 million queries Lumu detected and helped them quickly contain compromises in the first stages of the cyber kill chain, mitigating all impact to the organization.

As a top healthcare provider, they have more and more IoTs connected to their network. With Lumu they can monitor those assets and be sure that their patients' personal health information is protected and that an attack that could disrupt the business is not in progress.

After years of investment in cybersecurity, they now know what tools are working as expected and which ones need tuning to unlock their potential, all this with factual data provided by Lumu.

"We know that the healthcare sector is a big target for cybercriminals. The trust our patients place in us cannot be broken and that is why we were looking for a solution that will help us improve our cybersecurity posture. Now with **Lumu**, we can know at any time if a device has been compromised and take the necessary actions in a precise and timely manner."

CONTACT LUMU
SALES@LUMU.IO

www.lumu.io