HYAS

CASE STUDY

ALMO RESPONDS WITH HYAS™ INTELLIGENCE SERVICES

COMPANY AT A GLANCE

Almo (www.almomilk.com.au) was founded in 2015 with the mission of producing Australia's first long life Australia-grown almond milk. Almo is synonymous for quality and simplicity and continues to evolve and create a new generation of plant-based products.

CHALLENGES

- Rapid response to breach of cardholder information in midst of global Covid-19 pandemic
- Lean team without deep IT security and threat intelligence expertise

RESULTS

- Rapid investigation response limited damage and allowed focus on recovery
- Identified attacker located in Russia
- Enumerated the number of compromised records for precise breach notification

> The HYAS speed of investigation was incredible. We were blown away by responsiveness, knowledge and expertise. To rapidly identify security issues in our infrastructure as well as find the culprits was astounding. HYAS jumped in and located the hacker in hours. HYAS is the best staff we have ever connected with in cybersecurity globally.

Linda Monique, Chief Executive Officer, Almo

ENCOURAGING HEALTHY LIVING

Almo, located in South Melbourne, Australia, is an innovative manufacturer and distributor of clean, sustainability grown and produced almond milk to Australia and the Asia Pacific region. While much of Almo's operations focus on retail and export to international customers, the Coronavirus pandemic resulted in Almo focusing its energies on B2C e-commerce to grow its business. Linda Monique, CEO of Almo, commented, "As Covid-19 spread around the world, we started thinking of a strategy to adapt to the changed marketplace. International borders were closing and the traditional food service route was shuttering."

Almo had the added challenge of perishable inventory that could spoil if it was not moved promptly. Almo created a consumer promotion for Australia to leverage inventory and used an e-commerce strategy to reach Australian's university student population, a prime target demographic of consumers.

THE ORIGINS OF A BREACH

A challenge for all businesses moving online, particularly with the rapid economic change caused by Covid-19, is that their attack surface expands dramatically. This change results in new risks that do not become evident until after the attack. As the Australian Competition and Consumer Commission reported in the beginning of the Coronavirus pandemic, Australia had more reports of phishing attempts in April 2020 than in any previous month[1].

As Almo's online promotion progressed, Almo started receiving email and social media communication from customers regarding fraudulent transactions. Realizing that something was amiss, the team shut down Almo's e-commerce operation and started looking for security resources to help respond to the incident. To investigate the breach, Almo turned to HYAS.

INVESTIGATING AND RESPONDING TO THE INCIDENT

HYAS Intelligence Services responded within hours of being engaged. The HYAS team, which uses tools such as HYAS Insight, promptly identified the source of the breach as well as the number of customer records that were potentially compromised.

The HYAS Intelligence team had investigated attacks leveraging Magecart scripts previously, and after seeing tell-tale signs, quickly concluded that Almo had suffered from a Javascript injection typical of a Magecart attack. The malicious script installed by the adversary had exfiltrated a host of fields which would allow the actor to sell the stolen cards and conduct additional fraud, victimizing Almo's customers. Indicators of compromise (IoCs) in Almo's telemetry allowed the HYAS team to identify that a Russian adversary was behind the attack.

PROACTIVE DISCLOSURE

The Almo team worked with HYAS to understand the magnitude of the breach and best practices in responding. The firm had obligations to both its customers and to regulatory authorities to respond to the breach. Commented Monique, "We needed to manage brand reputation and the consequences of the hack. HYAS was able to identify the magnitude of the compromise so we could provide honest and verified information to customers that were affected. HYAS also provided a number of recommendations that we could immediately implement to improve our e-commerce security."

In addition to notifying affected consumers, Almo worked with Australian authorities to report the data breach as well as notify law enforcement so they could pursue the culprit. The precise attribution provided by HYAS provided Australian law enforcement with detailed evidence from which they can pursue the suspect.

Summarizing the experience, Monique commented, "When you are in the midst of a breach, you have a bunch of unknowns. HYAS established trust and their investigation quickly provided details that we needed. Their rapid investigation response identified how many records were exposed, the location and identity of the attacker, and what we needed to do to recover. It eased our minds and speeded the response to our valued customers and to the authorities."

---

[1] *Sydney Morning Herald, "Super scams, fake puppies: COVID-19 isolation triggers jump in cybercrime" 20 May 2020* https://www.smh.com.au/technology/super-scams-fake-puppies-covid-19-isolation-triggers-jump-in-cybercrime-20200519-p54ued.html

FOR MORE INFORMATION OR TO SCHEDULE A DEMO, PLEASE CONTACT US AT:

Email: info@hyas.com
Web: hyas.com/demo
Phone: +1-888-610-4927

ABOUT HYAS™

Founded by a team of world-renowned security researchers, analysts and entrepreneurs, HYAS is a highly skilled information security firm developing the next generation of information security technology. HYAS enables enterprises to detect and mitigate cyber risks before attacks happen and identify the adversaries behind them. HYAS Insight is a threat intelligence and attribution platform that improves visibility and productivity for analysts, researchers and investigators while vastly increasing the accuracy of their findings. HYAS Insight enables analysts to connect specific attack instances and campaigns to billions of historical and real-time indicators of compromise faster than ever before, bringing invaluable new intelligence and visibility to security efforts. Threat and fraud response teams use HYAS Insight to hunt, find, and identify adversaries, often down to their physical doorsteps. To learn more about HYAS, please visit https://www.hyas.com .