CYFIRMA
DECODING THREATS

INDUSTRY
Discreet Manufacturing

SOLUTION
Threat Visibility and Intelligence Module

BENEFITS
Early warning system gave valuable insights into the emerging threats, attack, motives and methods, allowing client to take actions to prevent data breach

Large Manufacturing Company Averted Corporate Espionage with Predictive Threat Intelligence

The manufacturing plant has a global footprint across all continents. Its products are designed for both businesses and consumers. In order to manufacture the end-product, there is a long list of parts and equipment it needed to procure from many suppliers. Besides assembling the final product, this manufacturing plant has also invested heavily in R&D to find new ways to increase the value and use cases of the final product. Part of the R&D efforts involve using AI, cognitive computing and IoT to completely transform how the final product would perform to improve the lives of millions of people.

GO TO THE HACKERS' TRENCHES

CYFIRMA was hired to help the company monitor for cyber risk and to provide real-time intelligence. CYFIRMA's threat discovery and cyber intelligence platform revealed some disturbing findings which required immediate attention and remediation. Monitoring the dark and deep webs, surface web as well as various closed communities over a 24-hour timeframe, the platform uncovered conversations in the hackers' communities where the groups were planning to mount a cyberattack to exfiltrate intellectual property from the Large Manufacturing Company's R&D.

The intelligence further revealed the hacker groups were known to be state-sponsored, specifically by the Korean and Chinese government. The objective was to gain access to the data on the plant's IoT research as the asset can be of value to competing nations who are racing to develop similar technology.

The method discussed was to exploit a vulnerability in the Large Manufacturing Company's supplier management system. The supplier portal was accessible to third-party users, beyond the company's employee base. The Hackers would attempt to hack into the supplier portal using a vulnerable web application.

STAY A STEP AHEAD

The intelligence collected was critical in enabling the Large Manufacturing Company to understand the threat actors, their motive as well as the technique they intended to deploy to steal data. Other than providing full context with relevant intelligence, the report also gave a set of prioritized recommendations which the Large Manufacturing Company could quickly implement. In this case, the recommendation was to performance a patch update on the vulnerable web application, review the supplier management system and process, followed by updating the incident management process in the event a breach occurs.

This case study illustrates the immense challenge faced by security teams who often find themselves falling behind, left to analyse artefacts from the past to try to determine the future. The key to preventing a data breach lies in a holistic and comprehensive cybersecurity approach where threat intelligence would reside at the heart of a cybersecurity strategy. Organizations have attempted to introduce threat intelligence into their security tooling in order to detect and protect against known malicious domains, blacklisted internet addresses and other identifiers.

This intelligence consisted of millions of indicators that needed filtering and prioritising and were soon out of date. The challenge, thus, lies in obtaining quality threat intelligence – where the insights provided are relevant, prioritized and predictive.

CYFIRMA's early warning systems give clients the advantage of staying ahead of the game by predicting upcoming cyberattacks, and gaining insights into the emerging threats, attack, motives and methods. This approach presents risks and threats indicators at the planning stage as opposed to the execution and exploitation phase of a cyberattack.

To learn more, visit **CYFIRMA.COM**

About CYFIRMA

CYFIRMA is an external threat landscape management platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver early warning, personalized, contextual, outside-in, and multi-layered insights. Our cloud-based AI and ML-powered analytics platform provides the hacker's view with deep insights into the external cyber landscape, helping clients prepare for impending attacks.

CYFIRMA is headquartered in Singapore with offices in APAC, EMEA and the US. The company is funded by Goldman Sachs, Zodius Capital, and Z3 Partners.

CYFIRMA
DECODINGTHREATS

twitter.com/cyfirma
facebook.com/Cyfirma/
linkedin.com/company/cyfirma
www.cyfirma.com