CYFIRMA
DECODING THREATS

INDUSTRY
Global IT Services Company

SOLUTION
Threat Visibility And Intelligence Module

BENEFITS
- Early understanding of looming threats using detailed external threat landscape
- Proactive defense with quick identification of known or unknown threat vectors
- Complete context of threat with real-time correlation of key threat attributes
- Prevented exfiltration of customer data and averted financial and regulatory penalties

Comprehensive Threat Intelligence To Protect Customer Data

Running a global business operations across 50 countries, this IT Services Giant manages large-scale government and commercial contracts that often span over a number of years.

Its hybrid cloud network contains a large volume of customers' data such as employee particulars, payroll details, ERP, CRM and individual project plans.

As business expands and the number of service engineers increases, more employees have access to sensitive data. The IT Services Company was concern with its cybersecurity posture and resiliency as any data breach could result in legal action from its clients.

INTELLIGENCE-CENTRIC

CYFIRMA's threat visibility and intelligence module detected conversations in hacker's forums where there were interest on this IT Services company's customers' information, particularly, IT implementation project plans, architecture documents, IT infrastructure schema and other sensitive data.

CORRELATING THREAT ACTORS, MOTIVES, CAMPAIGN AND METHODS

CYFIRMA's early warning detection system also noted the motive of the hacker group was to exfiltrate the confidential data and sell it on the dark web marketplaces.

CYFIRMA monitored the deep and dark web, hackers' forums, surface web, and closed communities to uncover a variant malware which was used previously by other hacker groups to launch a cyber attack against this IT Services Company.

Having identified the indicators of compromise (IOCs) for the malware strain, CYFIRMA also analyzed other associated IOCs related to the overall campaign.

STRATEGIC, MANAGEMENT AND TACTICAL INTELLIGENCE

By understanding external threat landscape and hackers' interest towards customer information and their respective master IT implementation plans, the Global IT Services Company's security management team updated the company's Data Loss Protection Policy to monitor and block sending of key documents outside of the organization.

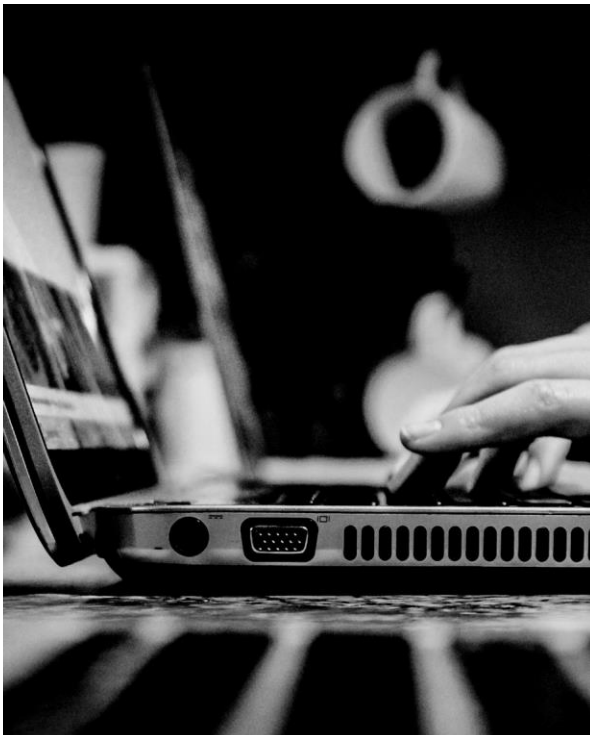
The security operations team was able to block the new malware strain from entering the Global IT Services Company's firewall, proxy servers, and EDR solution.

With the intelligence and insights provided by CYFIRMA, the Global IT Services Company also activated additional IOCs on its SIEM solution. This facilitated the monitoring of the malware, and allowed the SOC team to understand if any connections were made to the external command and control center.

CONSEQUENCE

Should the hackers have successfully entered the IT Services Company's environment and stolen its client's data, the consequences would be unbearable.

The customer data would have revealed confidential trade secrets, digital transformation strategies and full schemas of IT infrastructure, network, systems and applications. And likely to result in hefty financial penalties and lawsuits.



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

About CYFIRMA

Headquartered in Singapore and Tokyo, CYFIRMA is a leading threat discovery and cyber-intelligence platform company. Its cloud-based AI and ML powered platform helps organizations proactively identify potential threats at the planning stage of cyberattacks, offers deep insights into their cyber landscape, and amplifies preparedness by keeping the organization's cybersecurity posture up-to-date, resilient, and ready against upcoming attacks.

CYFIRMA works with many Fortune 500 companies. The company has offices and teams located in Singapore, Tokyo, and India.

CYFIRMA
DECODING THREATS

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