CYFIRMA
DECODING THREATS

Midsized Company Staves Off Third-Party Risk from Supply Chain Partners with CYFIRMA's Digital Risk Protection Platform – DeTCT

COMPANY
Midsized Firm

INDUSTRY
Industrial & Wholesale Distribution

HEADQUARTERS
Asia

SOLUTION
DeTCT – Digital Risk Protection Platform

CHALLENGES

- Interconnected nature of business means digital risks are extended to firm's supply chain; hence essential to limit business disruption caused by breaches in supply networks
- Rising exposure to 3rd-party risk due to increasing partners and vendors in supply chain
- Limited skilled cyber resources restricts ability to zero in on real risks and remediations
- Need to focus on business growth than be distracted with new / growing attack surfaces

BENEFITS

20X
Faster Threat Hunting Speed

USD$30M
Losses Averted

Avoided
Massive Breach, Significant Legal Liabilities and Reputational Losses, and Business Disruption

ABOUT THE COMPANY

This midsized company is involved in the trading of industrial machinery and components as well as the wholesale distribution of industrial equipment in Asia Pacific. A leading player within its segment, the company has been growing rapidly and has an annual turnover of around US$80 million.

THE CHALLENGE

As a midsized industrial firm in a competitive sector with many bigger players, the company has been going through digital transformation to drive productivity and efficiency as well as improve safety. Through digitalization, the firm also sought to enhance decision-making through data-driven insights.

As a result, the company's supply chain is no longer linear; instead, it is interconnected, giving the company the ability to swiftly respond to changes in demand and supply.

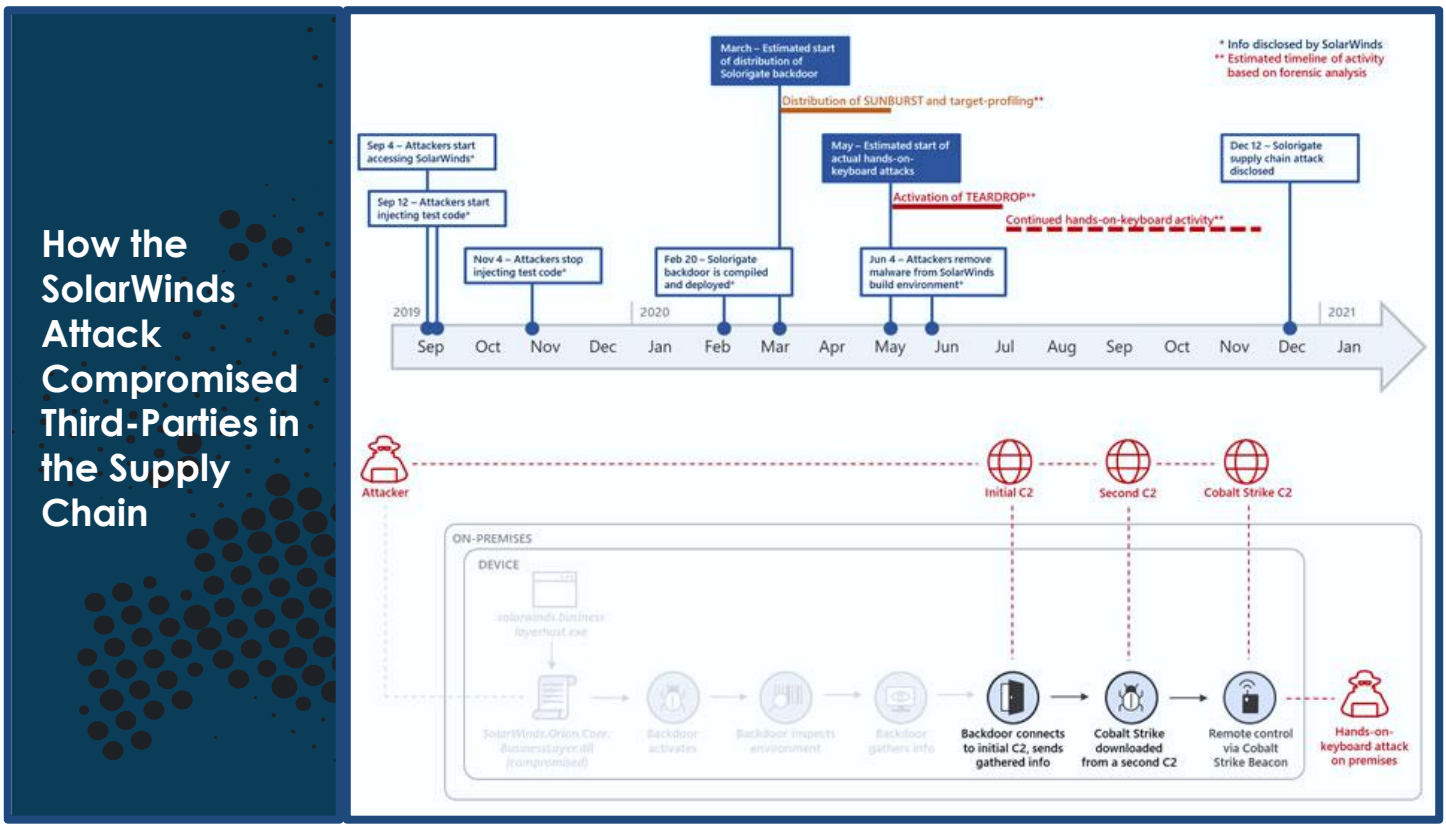
However, having an agile supply chain also means the industrial firm's exposure to third-party digital risk is at high-speed: Anything that its supply chain partners get exposed to can very quickly compromise the firm too.

"40% of security breaches now stem from indirect attacks against weak links in the supply chain. That's very concerning. **With DeTCT, we are now proactively safeguarded from these third-party risks so we can focus on what matters – our business and customers.**"

CEO, Midsized Industrial Firm

"DeTCT has given us the ability to build our own centralized, highly relevant third-party threat intelligence in-house. Now, we can proactively defend our proprietary and customer data."

CIO, Midsized Industrial Firm



At the same time, the industrial firm also found its supply chain expanding due to business growth. With an increasing number of third-party partners and vendors who can access its business applications, networks and data, the company knows it must closely monitor the network of suppliers that drive their operations.

Furthermore, the industrial company's management learned about the SolarWinds attack, a massive cybersecurity attack in 2020 that spread to its customers and partners, including elite cybersecurity companies, upper echelons of governments, and nongovernmental organizations.

Its C-suite were alarmed and felt the need to seek a superior solution to help them prevent scenarios like this.

HOW CYFIRMA HELPED

The midsized industrial company wanted to proactively safeguard against third-party risks that can occur due to weak links in the supply chain. With a complex supply network comprising multiple vendors and sub-tier suppliers, it needed to be able to map the risks not only from the third-party partner, but also the fourth, fifth and more, till the Nth-tier.

The management also wanted a comprehensive view of its digital risk status, plus trustworthy advice on how exactly to remediate any vulnerabilities for maximum protection against cyber threat actors.

They discovered CYFIRMA's DeTCT digital risk protection platform suited the company both in terms of capabilities and value.

The industrial firm subscribed to DeTCT, and it was promptly deployed at the company within hours.

DeTCT instantly uncovered backdoors and potential corporate espionage.

Almost immediately, DeTCT determined the industrial firm's digital footprint and attack surface, including its third-party risk exposure across the company's entire supply chain.

DeTCT's initial discovery unveiled a few critical breaches:

Backdoors. Several backdoors were allowing spies access to the company's proprietary information and data. Delving deeper, DeTCT uncovered that the backdoor was created through a hacked code that infiltrated one of its vendor's software updates.

Hacker exposed assets indicated potential corporate espionage. As a result, there were several hacker exposed assets including the company's distribution channels and upcoming distribution plans. These plans were critical to

"**DeTCT's ability to map digital risks to the Nth tier within our supply chain has helped us work more productively with our partners**. We have been sharing vulnerability intelligence with vendors, suppliers, and partners. They appreciate it. And we're able to create a more resilient supply ecosystem."

Head of Supply Chain, Midsized Industrial Firm

a planned strategic investment to grow its distribution channels in a particular region.

WHY IT MATTERS: DeTCT's insights highlighted the breaches almost immediately. This allowed swift action for the company's IT department to make urgent remediations to contain the damage.

As a result of DeTCT's discovery regarding the potential corporate espionage, the industrial firm did not go ahead with the expansion plan. The management assessed that the investment would not have likely given them the desired returns due to compromised data. This saved the company US$30 million in a deal that would likely go awry.

DeTCT unveiled third-party risks from vendor, thereby averting massive breach, legal and reputational losses, and business disruption.

Complete visibility of attack surface. DeTCT revealed the 'doors' and 'windows' into the industrial firm, together with potential attack routes from its supply chain ecosystem.

The comprehensive attack surface DeTCT shown included the firm's domain vulnerability, certificate weakness, configuration issues in DNS/SMTP/HTTP, open ports, IP/domain reputation, and cloud weakness, among others.

With this information combined with DeTCT's continuous monitoring of the dark web, surface web and social media 24/7, DeTCT was able to attribute substantial digital risks to one of the industrial company's vendors, V.

Upon discovery, a prioritized alert combined with recommended actions was sent to the relevant stakeholders of the industrial company immediately. The alert disclosed that the risks stemmed from several vulnerabilities in V's system and suggested the exact actions to take as critical next steps.

WHY IT MATTERS: Prompted by DeTCT's insights, the industrial firm acted based on the recommended remediations, which allowed swift response. It also communicated the weaknesses with V, who immediately took action to remediate its exposures to cybercriminals.

Left unaddressed, V's weaknesses would have resulted in an escalating breach, which would compromise the industrial firm's entire IT infrastructure in months. With multiple networks penetrated, it would have been very expensive and difficult to secure systems then.

The system compromise would also have caused severe legal liabilities and reputational losses to the industrial firm.

DeTCT built stronger relationship with supply chain partner by sharing vulnerability intelligence.

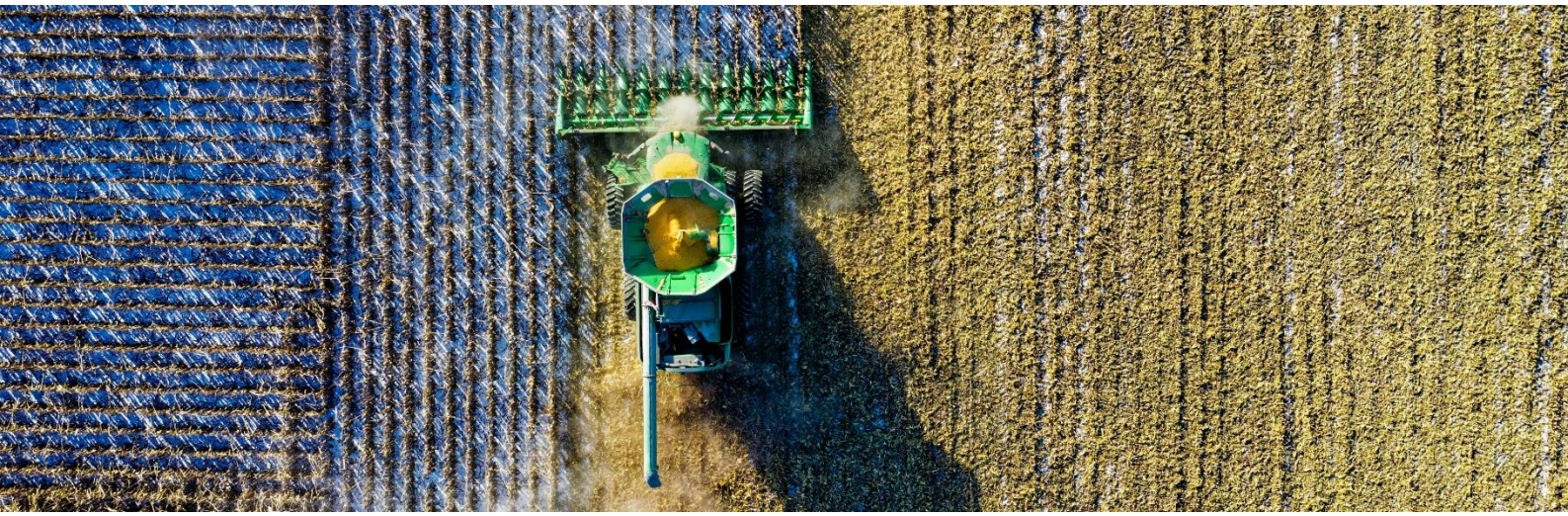
Sharing vulnerability intelligence with partners. DeTCT's ability to reveal third-party risks meant that the industrial firm was able to communicate these insights with its supply chain ecosystem.

In this case, DeTCT uncovered a range of digital assets belonging to the industrial firm's partner, P, in the dark web and several hackers' forums. These included domains, sub-domains, and IP addresses

The industrial firm shared DeTCT's vulnerability intelligence with P, revealing that P's key data had been exfiltrated.

WHY IT MATTERS: The sharing of DeTCT's vulnerability intelligence promoted a more robust and cyber-resilient end-to-end supply chain ecosystem. It also strengthened the working relationship between the industrial firm and P, resulting in a more enduring partnership.

Cementing strong partnerships is a particularly important aspect for the industrial company's continued stability and growth. This is especially amid the pandemic where supply networks are volatile and business conditions are uncertain.



PEACE OF MIND WITH SUPERIOR THIRD-PARTY RISK MANAGEMENT

Today, the industrial firm harnesses DeTCT to reveal new attack surfaces 24/7. Whether it is systems vulnerability, data leaks, or brand infringement and executive impersonation attempts, the company is now empowered to anticipate threats and stay ahead of third-party, supply chain related risks.

DeTCT protects brand integrity with brand intelligence.

The earlier exposure of backdoors and potential corporate espionage reinforced the firm's commitment to protect the company's brand. In today's already uncertain environment, its C-suite knows that customers' confidence will be eroded by cyberattacks, especially those that result in brand infringement, executive impersonation, or customer data exfiltration .

With DeTCT's brand intelligence, the firm now routinely assesses all online entities potentially masquerading as its business digital profile, assets, products, or brand - based on its domain name. DeTCT also alerts the company if ever its brand is under attack.

This proactive approach gives the management peace of mind that it will receive the most comprehensive information to circumvent any malicious acts in the planning.

DeTCT helps industrial firm stays ahead of threat actors with real-time monitoring.

With DeTCT's real-time attack surface discovery, the industrial firm now readily identifies porous or shadow IT systems that can be accessed by cybercriminals.

The spectrum of insights offered include how each asset and its gaps are being lined up for a possible cyber kill-chain exploitation.

In addition, the industrial firm also receives the latest vulnerabilities and contextual information mapped to its business and supply chain partners' assets.

This live awareness enables the firm's management, IT department, and security operations teams to conduct a realistic cost-benefit analysis of each asset. And decide how to shrink its attack surface in real-time, to stay ahead of malicious threat actors.

DeTCT's risk ratings and recommended actions = accurate resource prioritization.

DeTCT's alerts, which are categorized with risk ratings and recommended actions, now continues to help the industrial company take a risk-based approach to triage. It shows the severity of exposure (with Risk and Hackability Scores), along with effective remediation options that highlights exactly the 'where' and 'how'.

These relevant and prioritized updates 24/7 allows the firm's respective teams to act on vulnerabilities and indicators of compromise (IoC) pertinent to the industrial machinery and wholesale distribution sector and the region it operates in.

This has been immensely helpful as the firm discovered that decision-making can be stressful when dealing with potential cyber breaches.

With DeTCT's methodical flagging of risks and recommended actions, the industrial firm is now confident of acting in the most effective and efficient manner to contain the consequences in the event of a malicious attack – the only way to minimize the fallout.

About CYFIRMA

CYFIRMA is a threat discovery and cyber-intelligence platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver predictive, personalized, contextual, outside-in, and multi-layered cyber-intelligence. We harness our cloud-based AI and ML-powered analytics platform to help organizations proactively identify potential threats at the planning stage of cyberattacks. Our unique approach of providing the hacker's view and deep insights into the external cyber landscape has helped clients prepare for upcoming attacks.

CYFIRMA works with many Fortune 500 companies. The company has offices located in the USA, Japan, Singapore and India.

Visit https://www.cyfirma.com/ today

CYFIRMA

DECODING THREATS