CYFIRMA
DECODING THREATS

Food & Agri-business Countered Digital Threats with CYFIRMA's Digital Risk Discovery Platform DeTCT

COMPANY
Global Retail Company

INDUSTRY
Retail

HEADQUARTERS
North America

SOLUTION
DeTCT – Digital Risk Discovery and Protection Platform

CHALLENGES

- Brand infringement coupled with data exfiltration attacks
- Need a holistic overview of digital footprints and attack surfaces
- Counter emerging threats and leverage digital risk protection to reduce risk level

BENEFITS

3X
Drop in Incident Rates

12X
Improved in Speed of Remediation

Prevented
Data exfiltration which would have caused untold damages

ABOUT THE COMPANY

The client is one of the largest food and agri-business company in Asia, operating in 20 countries and supplying food and industrial raw materials globally. The company owns plantations producing palm oil which in turn is used in many food products.

The company's growth is highly dependent on its palm oil production, supply chain health, and commodity trading.

THE CHALLENGE

As part of its effort to improve efficiency throughout its entire ecosystem, the company embarked on a digitalization process to track the health of its plants and use data analytics to forecast output. The project has direct business impact as the data would guide and influence commodity prices. The project also resulted in employees who were accustomed to traditional way of operations having to learn new digital skills.

The onset of the COVID-19 pandemic compounded the problem when employees had to shift to a work from home model where they were accessing corporate data outside the security framework of the corporate network.

When the company started to see a number of websites with domains that look like the official site and employees were receiving an onslaught of phishing emails, the business knew cyber threats were looming.

"The digital risk discovery capabilities has helped us understand our security gaps on a real-time basis and this has allowed us to address emerging issues before we are subjected to greater risk."

CIO, Large Food and Agri-Business Firm in Asia

HOW CYFIRMA HELPED

The food and agri-business company approached CYFIRMA to assess its security posture and risk profile, understand threats posed by targeted as well as opportunistic cybercriminals, minimize overall risk, and protect its customers, clients, and employees.

The firm was onboarded to DeTCT and within 24 hours, DeTCT was able to highlight critical blind spots and uncovered threats that had remained unnoticed for days.

Blind Spot #1 – Impersonation and Infringement

DeTCT helped the company curb phishing attempts and highlighted websites abusing the brand name for financial gains. Attackers frequently set up fake websites using look-a-like domains offering counterfeit goods and services under the brand name and in some cases hosted phishing kits to steal sensitive data from unsuspecting users. These threats kept popping up in great numbers on a daily basis causing enough damage even before security teams could be alerted.

WHY IT MATTERS: Domain names are central to the identity of a business and hence are a lucrative target for cybercriminals. The lack of adequate protection and monitoring strategies for domain names and the brand as a whole lead to web traffic diversion, customer confusion, loss of trust, sale of counterfeit goods and services, phishing attacks, and even the distribution of malware.

Since it is not feasible for a business to buy endless potential domain name variations, having a monitoring solution to uncover spoofed domains in real-time is an important capability.

Blind Spot #2 – Compromised User Credentials

DeTCT discovered a decommissioned endpoint of the R&D department was left unsecured and exposed sensitive details of employees. The company's IT team also noticed brute-force and abnormal login attempts to critical applications.

Using DeTCT, it was brought to the client's attention that numerous compromised user credentials related to critical IT systems were being circulated in underground marketplaces and data leak sites.

WHY IT MATTERS: DeTCT flagged the compromised user credentials almost immediately, allowing security teams to take rapid action and prevent credential abuse which could have snowballed into an adverse event.

Undeniably, abuse of compromised credentials has remained one of the popular initial attack vectors and provides a low barrier to entry for motivated hackers.

With ransomware attacks gaining momentum, cybercriminals are continuously using exposed user credentials for quick and easy access to corporate environments to steal data and extort ransom.

Blind Spot #3 – Attack Surface Discovery

Due to its global presence and numerous third-party solutions being utilized, it was a challenge to discover, classify, prioritize, and monitor external assets. With employees working from home and without the protection of the corporate network, attack surfaces were also increased.

While implementing the digitalization project to forecast harvest output, a number of development cloud instances were created, and these were left unsecured when the project was completed. DeTCT discovered these cloud instances contain weaknesses that can be compromised by hackers.

The client utilized DeTCT to get an overview of all their digital assets including domains, subdomains, IP addresses and certificates. DeTCT also proceeded to identify vulnerable systems and misconfigurations in externally exposed assets.

WHY IT MATTERS: Managing attack surface is critical for organizations as it enables IT and security teams to discover, classify and assess the security posture of attacker-exposed assets.

By leveraging DeTCT, the company gained visibility into known/ unknown, secure/ vulnerable, active/ inactive digital assets and knew exactly which vulnerabilities needed to be fixed.

Blind Spot #4 – Dark Web Monitoring

DeTCT was able to pick up data leaked in dark web marketplaces and available for sale. The food and agri-business' networks were listed in the target list of a planned DDoS attack. Additional investigation revealed the planned attack was part of a hacktivist campaign targeting companies deemed to have profited from de-forestation.

With this insight, the client swiftly configured its firewall to block out the malicious IPs and prevented an attack.

WHY IT MATTERS: Dark web forums and marketplaces provide cybercriminals a discreet cover where they engage and plan their attacks. It is a place for like-minded cybercriminals to freely exchange resources including trade of corporate access, business-critical data, valuable data such as PII, exploit details, etc.

With DeTCT, the client could effortlessly tune into a broad range of dark web sources efficiently.

Using DeTCT to identify 'doors and windows' which hackers can use to break into the environment.

Today, the food and agri-business firm relies on DeTCT to continuously monitor for new attack surfaces, uncover vulnerabilities and digital threats.

The real-time continuous monitoring capabilities to identify shadow IT or porous systems which can be accessed by cybercriminals is key to identifying risk and threats at the earliest possible. Awareness of the attack surface has allowed the company to conduct a realistic cost-benefit analysis of each asset and decide how to shrink their attack surface.

Using DeTCT, the IT and security teams have been able to uncover the following:

- Domain vulnerability
- Certificate weaknesses
- Configuration Issues in DNS/SMTP/HTTP
- Open Ports
- IP/domain reputation
- Cloud weaknesses
- Vulnerabilities in external assets

The food and agri-business company continues to drive innovation across its entire business knowing that DeTCT is there monitoring their digital risk 24/7.

Know when their brand is under attack
- How is the brand being targeted?
- Comprehensive view of brand, product, solution infringement

Clarity on digital profile, data leaks, breaches, and impersonations
- Domain, IT Assets Impersonation
- Executive/People Impersonation
- Lookalike Social Handlers

Social and Public Exposure
- Confidential Files
- Source Codes
- Dumps of PII/CII
- Malicious Mobile Apps
- Negative Social Sentiments

Real-time data breach monitoring
- Email, identities, credential leaks
- Intellectual Property
- Personal Data
- Dark web
- Database exposure
- Financial Leaks and Carding

To learn more about DeTCT™ and CYFIRMA, visit **WWW.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 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
DECODINGTHREATS

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