CYFIRMA
DECODING : THREATS

Global Financial Group Averts M&A Disaster with CYFIRMA's Threat Discovery and Cyber-Intelligence Platform

COMPANY

Global Financial Services Group

INDUSTRY

Banking & Financial Services

HEADQUARTERS

Asia

SOLUTION

DeCYFIR –Threat Visibility and Cyber-Intelligence Platform

CHALLENGES

- Situational awareness exercise for M&A uncovered corporate espionage
- Needed to contain damage and limit fallout due to breach

BENEFITS

12X
Increase in Threat Hunting Speed

16X
Faster Remediation Speed

USD$400M
Cost Savings

Avoided
M&A Fiasco & Share Price Plunge

ABOUT THE COMPANY

The leading global financial services group is one of the largest banking institutions in Asia. The institution's capital stands at around USD$10.4 billion as of 2021 and is one of the main companies of a larger conglomerate. As part of its business, the Financial Group pursues mergers and acquisitions (M&A) to develop strategic business advantages.

THE CHALLENGE

While M&As can help companies create strategic value, cybercriminals and nation-state threat actors view these market-moving activities as attractive targets due to the substantial capital typically involved.

Hackers engaged for corporate espionage can target confidential, carefully deliberated positions to weaken the competitor's hand in negotiation. The M&A transaction itself can also be targeted by threat actors looking to profit from trading secret M&A data on the dark web, or by exploiting financial markets.

The Financial Group was in the process of evaluating an African coal company for acquisition to diversify its business portfolio. To gain better situational

> "The digital risk discovery capabilities helped us uncover our attack surfaces rapidly, so we know the security gaps we need to address."
>
> SOC Team Leader, Global Financial Group

> "DeCYFIR allowed us to swiftly map a clear path to contain the damage caused by an episode of corporate espionage. As a result, we averted a potential M&A fiasco that could harm our brand and cause our share price to drop. We also saved USD$400M by cancelling the untenable deal."
>
> CISO, Financial Group

Hackers Hired for Corporate Espionage Targeted Global Financial Group

UNDER TARGET I Cloud Solutions I Cryptocurrency I Blockchain I Third Party Integrations I Robotics I AI / Machine Learning (ML) Enabled Systems I Connected IOT Communications I Online Transaction

EXPECTED DAMAGES

- PII/CII Data Exfiltration
- Compromised M&A Deal
- Financial Losses
- Brand Damage
- Share Price Impact

PROFILE I Suspected involvement of multiple mercenary, hacker-for-hire groups

RECENT ACTIVITY I APT, Phishing, Data Exfiltration Malware

MOTIVE I Financial gain, damage and disruption to business operations

awareness for the M&A process, the Group hired CYFIRMA to work with its due diligence team.

HOW CYFIRMA HELPED

The Financial Group wanted to assess the coal company's security posture and risk profile, determine cybersecurity threats early in the M&A process, and lower risk throughout the entire M&A process.

DeCYFIR™'s predictive threat intelligence capabilities swiftly detected corporate espionage.

As such, the Group subscribed to DeCYFIR™, the world's first predictive cyber-intelligence platform which was deployed rapidly in a few hours. Once operational, DeCYFIR™ instantly detected a social media leak of the Financial Group's bid-offer details.

The leaked details included the Financial Group's valuation of the coal company, its offer price, share price, bid proposal, employees to keep and to let go of, new organizational structure, and integration plan.

DeCYFIR™'s sophisticated predictive intelligence engine – which embeds virtual drones in deep/dark web forums and underground markets for continuous monitoring – also uncovered the leaked bid details of four other firms vying for the same coal company.

Alarmingly, DeCYFIR™ unveiled that the M&A broker listed was the same for these four other bidders.

WHY IT MATTERS: DeCYFIR™'s flagged the data leak almost immediately, allowing rapid action to contain the damage and minimize the fallout.

By unveiling the interest four other firms had in the coal company and connecting them to one M&A broker, DeCYFIR™ also helped the Financial Group understand the motive of the threat actors to better respond.

DeCYFIR rapidly uncovered attack surface and vectors.

With that knowledge, CYFIRMA instantly harnessed DeCYFIR's digital risk discovery's capabilities to determine the Financial Group's digital footprint and attack surface. This was critical for the Group's security team to map a clear path towards risk mitigation and prevent a recurrence of the breach and attack. It would also help limit potential damage to the Financial Group's brand, reputation, and finances.

DeCYFIR quickly revealed hacker-exposed assets other than the sensitive M&A data that was exfiltrated and discovered on social media. It detected several hijacked email accounts that were likely captured by multiple cyber hacking groups hired to obtain sensitive information so that the competing bidders can gain an unfair advantage in the M&A negotiations.

The attackers sent phishing emails targeting the company's senior executives. These emails, which were tailored to their chosen targets and used M&A-themed baits, lured the victims into opening attachments or clicking links that implanted highly sophisticated data exfiltration malware.

Visual Basic for Applications (VBA) macros were also implemented to steal the usernames and passwords of key individuals. Once the user's credentials were captured, the hackers likely obtained access to real-time email communications which offered insight into how the M&A deal was being structured.

In addition, DECYFIR exposed a range of digital assets such as domains, sub-domains, and IP addresses that had been compromised. These details were found in hackers' forums, the dark web, and several bin sites – which showed that malicious actors have found a way to breach the Financial Group's defenses and exfiltrated key data.

WHY IT MATTERS: The speed at which exposed digital risk is uncovered can determine the extent of the damage to brand, reputation, and finance.

By uncovering its full attack surface swiftly, DeCYFIR allowed the Financial Group's security operations center (SOC) teams to quickly work on reducing the company's attack surface with system hardening. This included regaining control of hijacked email accounts, as well as disabling unnecessary services, user accounts, and ports.

DeCYFIR revealed impersonation and infringement attempts.

DeCYFIR also exposed several fake identities of the Financial Group's top executives, including fake email IDs used in the phishing campaigns to trick employees into clicking malicious emails.

In addition, DeCYFIR uncovered brand infringement attempts consisting of multiple online entities masquerading as the Financial Group which were trying to deceive users into divulging personal information.

WHY IT MATTERS: By providing the background information, description, and impact for the impersonation and infringement attempts, DeCYFIR helped the Client's SOC team remediate these cyber risks instantly to limit further exposure. The SOC team also fortified defenses in these areas to prevent APT actors from regaining a foothold in the company's network following remediation.

DeCYFIR's risk ratings and recommended actions ensured cybersecurity resources were prioritized correctly.

From the point the data breach was detected, the Financial Group knew it needed to optimize the company's cybersecurity resources in a rapid and synchronized manner to contain the consequences.

DeCYFIR's alerts, which are categorized with risk ratings and recommended actions, helped its management and SOC teams take a risk-based approach to triage by showing the severity of exposure swiftly, along with effective remediation options.

WHY IT MATTERS: In an evolving threat situation, having the capability to direct precious cybersecurity resources to the right places is essential for minimizing impact.

DeCYFIR's alerts and dashboard which clearly highlights Risk and Hackability Scores along with recommended remediation actions showed the Client's team exactly the 'where' and 'how' for security triage.

DeCYFIR's trend indicators helped the Financial Group's leadership chart ongoing risk and exposure.

By delivering trend analysis across six key domains, namely, Attack Surface, Impersonation & Infringement, Data Breach Monitoring, Social & Public Exposure, Dark Web Exposure, as well as Vulnerabilities Exposure, DeCYFIR helped the Group's senior management monitor and stay ahead of the company's ongoing risk.

WHY IT MATTERS: The Financial Group's management was concerned about the breach and wanted to ensure the threat actors were not attacking other areas in the company. DeCYFIR's trend indicators helped them easily track ongoing security defense progress as well as exposure to new risks on a single dashboard.

CYFIRMA aided the Financial Group in reassessing its position to acquire the coal company: Saved USD$400M and avoided M&A debacle.

In the wake of the data breach, the Financial Group re-evaluated its decision to acquire the coal company, knowing that some, if not all, of the four competing bidders would likely have accessed its bid-offer details and knew how to gain an upper hand.

Further customized insights from DeCYFIR's predictive intelligence platform also suggested that the coal company's security posture may not conform to the Financial Group's standards and may compromise their network if the M&A was successful.

As a result, the Financial Group called off the purchase of the coal company, saving its offer price of USD$400 million. In doing so, the Financial Group also deflected an M&A disaster that could tarnish its reputation and risk its share prices plummeting.

WHY IT MATTERS: Had the Financial Group gone ahead with the deal, it would have grossly overpaid for the coal company.

Its share prices would have tumbled, and its brand affected in the aftermath as analysts discovered that the acquisition was overvalued. This could lead to a decrease in brand loyalty and lost revenue opportunities.

STAYING AHEAD OF THREATS WITH DeCYFIR™

Today, the Financial Group uses DeCYFIR™ daily to anticipate threats and combat potential attacks.

Multi-layered intel helps different organizational stakeholders get the insights they need.

With DeCYFIR™'s multi-layered intelligence tailored to different levels in the organization – specifically, strategic, management, and operations, The Financial Group's stakeholders across different levels have been able to make the right decisions concerning its risk exposure and attack surfaces.

Strategic: This includes answering the 'who', 'why', and 'where' questions regarding potential threat actors so the C-suite can update strategy, governance, and policy based on the threat intelligence.

Management: Insights that cover the 'where', 'when', and 'how' help the Financial Group's executive management such as CISO and CIO make necessary changes to processes and procedures.

Operations: For its SOC teams, intel to the 'how' and 'what' aspects are giving them critical information to update security controls and devices.

Contextualized insights provide unmatched knowledge into cyberattacks in the making.

With DeCYFIR™'s detailed risk dossier that highlights malicious threat actors, the campaigns they are launching, and attack methods, the Financial Group is gaining valuable insights to implement new policies and update its controls to stop cyberattacks in their tracks. This includes attacks currently in progress, as well as those which are in the making.

Outside-in, predictive threat intelligence pre-empts known or unknown threats.

Pre-emptive identification of threats from an outside-in perspective from both known and unknown threat actors and vectors has given the Financial Group insights into why it is an attractive target and its vulnerabilities that can be exploited.

This has helped the company predict cyberattacks and strengthen its overall security posture.

Accurate alerts to imminent attacks enable continuous adaptation.

DeCYFIR™ is also delivering prioritized, relevant and tactical mitigations for the Financial Group's SOC teams. Allowing them to act on vulnerabilities, indicators of compromise (IoC), and hashes pertinent to the financial services industry, as well as the Financial Group's technology and the geographies it is operating in.

This has allowed the SOC teams to keep its systems patched and remediate weak points which required immediate attention. More importantly, it enabled the Financial Group to continuously evolve its security defenses to block looming cyber assaults.

To learn more about DeCYFIR™ and CYFIRMA, visit WWW.CYFIRMA.COM

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