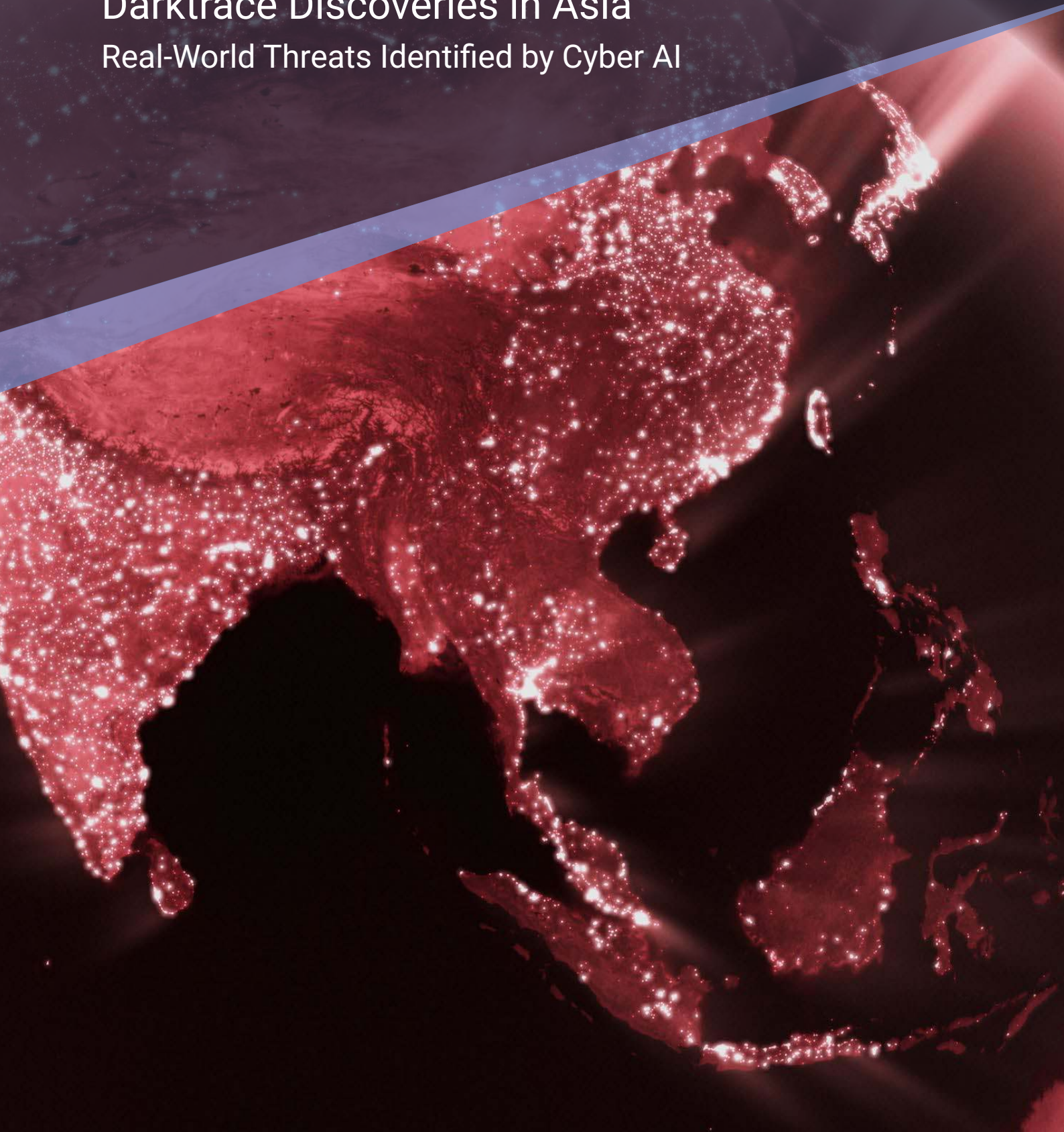
DARKTRACE

# Darktrace Discoveries in Asia

## Real-World Threats Identified by Cyber AI



# Introduction

Singapore's stewardship of ASEAN in 2018 made cyber resilience a top priority. Initiatives such as the ASEAN Cyber Capacity Program (ACCP) and the ASEAN Cybersecurity Cooperation Strategy aim to tackle the growing cyber-threat, while balancing the opportunities afforded by a digital economy. Strengthened cyber strategies, legislation, and research capabilities will be critical.

Organizations must take proactive steps to secure their digital business, or risk being left behind. Interconnectivity is driving change in organizations across enterprise and industrial environments. These advances come at the cost of heightened cyber risk. Even in less developed countries, the widespread implementation of IoT devices continues to blur the boundary between the physical and the digital. Consequently, these environments, and the devices in them, are vulnerable to exploit.

A joined-up cyber security strategy must at its core recognize that sophisticated threat actors will bypass traditional defenses at the network perimeter. Only this approach can tackle the breadth and sophistication of threats; from fast-moving attacks that damage businesses in seconds, before human security teams can respond, to slow and stealthy attacks which can lie undiscovered within a cloud or network system for months, perhaps even years.

AI performs this function, it is a fundamental ally in the battle against cyber-attacks. Autonomous response technology is a game changer because it fights back against threats in real time. As we move into an era of machine-on-machine battles, autonomous response will be vital in averting a headline-grabbing crisis.

Powered by artificial intelligence, Darktrace identifies and autonomously responds to threats that have bypassed the perimeter into an organization's infrastructure. Inspired by the human immune system, the technology learns a 'pattern of life' for every user and device. From this ever-evolving understanding of 'normal', the Enterprise Immune System identifies emerging threats that others miss. Darktrace Antigena then takes targeted, autonomous action within seconds to neutralize an emerging threat before it spreads.

As we move into a new age of cyber warfare, the defenders must shift the balance of power in their favor. By embracing world-leading cyber AI, organizations across Asia are, for the first time, gaining the advantage over today's ever-changing adversary – and winning.

# 1. Compromised Security Camera

**Industry:** Financial Services

**Point of Entry:** Internet-connected CCTV

**Apparent Objective:** Compromise an IoT camera as an entry point to the network

The increasing connectivity of everyday devices causes a big visibility problem for security teams. IoT devices, often with unintegrated, basic security controls, can be targeted by attackers who use them as stepping stones to a company's network.

At a Japanese investment consultancy, Darktrace discovered that an internet-connected CCTV system had been infiltrated by unknown attackers. In doing so, the perpetrators gained a foothold into the network, but could watch all of the camera's video recordings. Installed to monitor the entire office space, from the CEO's office to the boardroom, the camera instead became a security risk itself.

Darktrace AI quickly detected that something was amiss. Massive volumes of data were observed moving to and from the unencrypted CCTV server, as the attacker gathered data in preparation to exfiltrate sensitive information.

### Darktrace Antigena Fights Back

At the point when the attacker tried to exfiltrate the data, Antigena AI took rapid and precise defensive action. The autonomous response technology blocked any data moving from the device to an external server – while still allowing the CCTV to operate in its intended capacity.

The AI fought back at machine-speed, preventing a serious breach of market-sensitive information. Antigena gave the security team vital time to investigate and remediate before any harm was done.

# 2. Targeted Attack on Senior Executive

**Industry:** Financial Services

**Point of Entry:** Highly targeted attack against key executive

**Apparent Objective:** Exfiltrate sensitive information

At a financial services company in Singapore, Darktrace discovered a serious network compromise that could have resulted in the loss of millions of dollars. The discovery was made when Darktrace's AI uncovered network traffic being directed to an anomalous external destination. This was in fact a direct command and control channel between a bespoke implant and the attackers' infrastructure in South Korea.

Cyber-criminals had identified a specific senior manager, and launched a highly targeted and calculated attack. Having gathered information on the executive, the attackers crafted a phishing email containing specific, personalized details, such as recent travel, meetings, and people's names. They entered the corporate network via an attachment that, when opened, resulted in gaining remote code execution on the computer. The senior executive was compromised via a phishing email, but had no idea he was the victim of an attack.

The attackers gained full control over the executive's computer and access roles, using the device as an entry point to move laterally through the company's cyber infrastructure. Within minutes, they had scanned multiple devices throughout the network, searching for vulnerabilities. The criminals then exploited out-of-date software to install a remote access trojan.

The level of access the attackers achieved put them in an ideal position to cause systemic damage and undermine trust. For example, they had the potential to steal or tamper with confidential information in restricted file shares, deceive clients via emails, and even perform banking transactions. If Darktrace's AI had not discovered the breach at this early stage, the financial and reputational cost to the organization may have critically debilitated operations.

Although the hackers had evaded perimeter defenses, Darktrace's AI recognized the activity as malicious, compared to the organization's normal 'pattern of life'. Darktrace was able to detect the threat in real time, stopping the attackers before significant damage was done.

# 3. Phishing Scam Hijacks Manufacturer's Network

**Industry:** Manufacturing

**Point of Entry:** Malicious attachment sent via email

**Apparent Objective:** Exploit the corporate network for concealed phishing attacks

Whilst most cyber-attackers aim to steal or jeopardize data, a growing number of hackers seek to profit from hijacking a company's network infrastructure. This kind of attack is most commonly associated with cryptocurrency mining, but there are multiple, increasingly creative ways of exploiting this method of cyber-attack.

At a Hong Kong-based construction materials manufacturer, Darktrace discovered that the internal network had been exploited by cyber-criminals to conduct extensive and aggressive phishing attacks.

The breach occurred after an employee opened an email attachment containing malicious code. This common method of infiltration allowed perpetrators to compromise the employee's computer, and act as a parasite on the system's power and internet connection.

Criminals can then conceal their activity, preventing their IP addresses being discovered and making it easy to evade detection and possible prosecution.

The attackers attempted to use the hijacked device to send malicious emails to thousands of different addresses based in Russia. The emails appeared legitimate and were written in the recipients' native language, eliciting the victims to give them details about their bank accounts.

If not detected, the spam campaign would have led to the manufacturer's IP address being blacklisted, disrupting their ability to communicate via email. The effect on the supply chain would diminish operational functionality, business trust, and revenues. Thanks to Darktrace's ability to learn the 'pattern of life' for every user and device, it instantly recognized this behavior as a significant deviation.

## Darktrace Antigena Fights Back

Darktrace Antigena reacted within seconds to autonomously restrict traffic on the infected device. This prevented the emails from ever being sent.

While the malicious behavior was blocked, normal operations were able to continue. Because Darktrace Antigena fought back at machine-speed, the security team was able to gain back the time advantage and respond to the infection before any disruption was caused.

# 4. Major Attack Thwarted at IT Firm

**Industry:** Technology

**Point of Entry:** Software bug

**Apparent Objective:** Exfiltrate sensitive company information

Despite possessing advanced perimeter defenses, Darktrace's Enterprise Immune System discovered a threat within a Taiwanese IT company's network during the first week of its deployment.

On installation, Darktrace discovered existing malicious activity. The AI could still detect that the behavior was anomalous and flagged it to the company.

Cyber-attackers were exploiting a buffer overflow, a serious but well-known, form of software bug present in an application running on one of their servers. This enabled them to read adjacent memory and gain access to huge quantities of cached employee information used by the application.

This compromise had the potential to cause serious damage. Highly valuable, sensitive data was exposed via a routine attack. A continued exfiltration could have also put the company's customers at risk.

Darktrace's AI identified the attackers running scripts against the application as anomalous and flagged it to the company. The Enterprise Immune System's fast and precise detection of the breach allowed the company to take immediate action. This gave the company's security team the vital information and time they needed to avoid any further impact.

# 5. Encryption of 5,000 Documents Prevented

**Industry:** Financial Services

**Point of Entry:** Malicious attachment sent via phishing email

**Apparent Objective:** Encrypt crucial files and extort payment for decryption key

Ransomware remains one of the most serious cyber-threats. As new strains emerge every day, CISOs cannot afford to become complacent. Compounding the challenge, new regulations, like the EU's GDPR, have made the need for total visibility and control over sensitive information even more pressing.

At a technology and media investment company, an investment associate inadvertently downloaded a ransomware file after opening a malicious email attachment. The infected device then connected to the GandCrab ransomware infrastructure and instantly attempted to encrypt almost 5,000 internal documents, adding a document containing a ransom note demanding payment in order to unlock them. The moment the device downloaded the executable, Darktrace identified the threat as a sophisticated ransomware.

### Darktrace Antigena Fights Back

Darktrace Antigena blocked all outgoing communications from the infected device, stopping the infection in its tracks and preventing subsequent data loss.

Had Darktrace's AI not reacted within seconds, a large amount of highly sensitive financial information could have been encrypted. Due to the swift autonomous response against the machine-speed attack, the organization was spared tremendous financial losses and reputational damage.

## About Darktrace

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 3,000 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1000 employees and headquarters in San Francisco and Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.



## Contact Us

Asia-Pacific: +65 6804 5010

Europe: +44 (0) 1223 394 100

North America: +1 415 229 9100

Latin America: +55 11 97242 2011

info@darktrace.com | darktrace.com

@darktrace