# 2025 CYBERSEER SOC
# THREAT FINDINGS REPORT

Insights from our front line

CYBERSEER

In the first half of 2025, Cyberseer's SOC uncovered a wave of increasingly sophisticated attacks – blending stealth, speed and human ingenuity. This report details key adversary behaviours our analysts identified and the defensive measures that helped contain them.

Our findings underscore a critical truth: today's threats demand proactive detection, behavioural analysis and continuous investigation – exactly what Cyberseer's SOC delivers, 24/7.

## SOPHISTICATED PHISHING TACTICS

Adversary-in-the-Middle (AiTM) phishing attack campaigns use spoofed DocuSign portals embedded in SharePoint links and bypass MFA to harvest credentials. These attacks are tailored to deceive even vigilant users.

## RAPID VULNERABILITY WEAPONISATION

Exploits were observed in the wild within days after vulnerabilities were disclosed, reinforcing the urgent need for agile patch management and real-time threat monitoring.

## HUMAN-OPERATED INTRUSION

An increase in hands-on keyboard activity saw attackers dynamically adapting tactics in real time. These threats require expert SOC vigilance to detect and disrupt.

## STEALTHY MALWARE PERSISTENCE

PowerShell scripts linked to LUMMA STEALER malware attempted to persist via registry tampering – hiding in plain sight by mimicking legitimate system behaviour.

## ABUSE OF LEGITIMATE TOOLS

Remote monitoring and management tools like AnyDesk are being misused for lateral movement and data exfiltration. These "living off the land" techniques evade traditional detection but are exposed through behavioural analysis and anomaly detection.

## Download the full report

Explore the full range of threat trends and see how Cyberseer's SOC is accelerating detection and response.