Major Incident -1

Title	**Sality Malware Infection and Pirated Software Usage**
Finding/Observation	• Sality malware detected on multiple endpoints, associated with cracked software installations. • One internal system observed communicating with a malicious external IP (potential C2 activity). • No evidence of data exfiltration or operational impact identified.
Risk Identified	• Use of pirated and unauthorized software created a systemic malware entry point, significantly increasing enterprise-wide exposure to cyber threats. • Confirmed outbound communication with known malicious infrastructure exposed the organization to risks of remote attacker control and secondary payload deployment. • Incomplete endpoint security coverage and passive security configuration reduced the effectiveness of preventative controls and increased reliance on manual response. • While no data loss was observed, the control weaknesses identified materially increase the risk of future high-impact incidents, including data compromise and regulatory exposure.
Mitigation & Recommendation	• Affected systems isolated and malware removed through EDR scans. • Unauthorized software and PUPs removed from endpoints. • EDR configuration updated from Detect Only to Prevent Mode to strengthen threat prevention.

Major Incident - 2

Title	**Backdoor.ASP.BEHINDER Malware Detected**
Finding/Observation	• The security alert was triggered by the Endpoint Detection and Response (EDR) solution, Trend Micro Server & Workload Protection. The system detected the addpass.aspx backdoor within a temporary folder of the Internet Information Services (IIS) web directory. The file was being accessed by an external internet address originating from a network in China. • The external IP address was observed successfully accessing publicly available static application resources. • Although the traffic was allowed by the WAF and reached the backend server with HTTP 200 responses, the activity is consistent with automated reconnaissance or web crawling behavior rather than exploitation.
Risk Identified	• The attacker successfully navigated the dashboard , confirming that the compromised session for the TssSupport account remained active and valid. • The logs show a deliberate attempt to upgrade the communication protocol from standard HTTP to WebSockets and Server-Sent Events (SSE) via SignalR. This is a classic technique to bypass standard firewall timeouts and maintain a continuous Command and Control (C2) link • The rapid succession of "CheckModule" requests (AML, ETT, RR, Screening) suggests the attacker was using automated scripts or a web shell interface to map out the application's internal capabilities and sensitive data points. • Deployment via Bypass: The logs show the attacker utilized the /FileUploader/UploadFile endpoint multiple times to test and eventually drop the malicious payload, which was quarantined by EDR solution before getting executed.
Mitigation & Recommendation	• Isolated the affected system to contain and prevent further malicious activity. • Blocked the identified offending source IP address to prevent further malicious activity. • Implemented geofencing controls on the Web Application Firewall (WAF) to restrict traffic from unauthorized geographic locations. • Completed malware eradication and integrity verification of the affected server, including review of application binaries, web directories, scheduled tasks, services, and registry persistence locations, with no additional malicious artifacts identified. • Reset the Support account Password and informed not to use default credentials.