NOZOMI NETWORKS LABS

RESEARCH CONTRIBUTION TO THE OT-ISAC COMMUNITY

OT Threat Landscape

Manufacturing Sector

Q1 2026 · APAC Edition

WHITE PAPER

Prepared by Nozomi Networks Labs as a research contribution to the OT-ISAC community.
Source data: anonymized telemetry from participating APAC manufacturing environments, Q1 2026.

Table of Contents

Executive Summary

Across Asia Pacific, manufacturers face an evolving OT threat landscape, made worse by increased connectivity, expanding attack surfaces, and adversaries' sustained interest in critical infrastructure. According to the latest analysis from Nozomi Networks Labs, a clear pattern has emerged in APAC manufacturing: attackers are concentrating on discovery, credential access, and service-disruption techniques to gain footholds and interfere with operations.

Researchers analyzed anonymized telemetry from manufacturing environments in the first quarter of 2026 and found adversary activity focused on reconnaissance and availability-impacting actions, while malware trends and vulnerability exposure pose meaningful operational risk. In response, manufacturers should strengthen visibility, detection, and resilience to reduce exposure.

At a glance

~33% Discovery & scanning — the dominant attacker priority	**~23%** Denial-of-service & availability-focused activity	**~78%** Activity attributed to five state-associated actors
13.8% Brute-force credential attacks against exposed services	**>90%** Malware detections that are miners or trojans	**+9 pts** Higher share of HIGH-severity CVEs vs. global baseline

Among our top findings

- APAC manufacturing environments show a higher concentration of high-severity vulnerabilities than the global average.
- Discovery and scanning techniques account for approximately one-third of observed activity, making reconnaissance the dominant attacker priority.
- Brute-force credential attacks account for 13.8% of activity, underscoring persistent weaknesses in authentication controls.
- Denial-of-service and other availability-focused attacks represent around 23% of activity, making disruption a top adversary objective.
- Cryptocurrency miners and trojans together represent over 90% of malware detections.
- A select group of state-associated actors is responsible for roughly 78% of attributed activity, showing concentrated threat origins.

Introduction

The purpose of this research is to summarize the top threats targeting organizations in the Manufacturing sector across the APAC region in Q1 2026. We focus on the top techniques used by attackers, identify which malware was most prevalent in the region, and determine which vulnerabilities are currently affecting the associated

environments the most. All data used comes in the form of anonymized telemetry sent by participating manufacturing customers located in this area.

Top MITRE ATT&CK Techniques Used

Understanding which MITRE ATT&CK techniques appear most frequently across OT environments helps translate raw threat activity into actionable defensive priorities. By mapping observed behaviors to ATT&CK, defenders can move beyond indicators of compromise and focus on the tactics, techniques, and procedures (TTPs) that adversaries repeatedly rely on to gain access, evade detection, move laterally, disrupt operations, and maintain persistence.

This section highlights the top MITRE ATT&CK techniques identified in our analysis, with emphasis on the behaviors most relevant to industrial, critical infrastructure, and connected device environments. These techniques reflect where attackers are concentrating their efforts and where security teams can achieve the greatest impact by strengthening visibility, detection logic, segmentation, access controls, and response playbooks.

Technique ID	Technique Name	Tactic	Share
T0846	Remote System Discovery	Discovery	**16.6%**
T0841	Network Service Scanning	Discovery	**16.6%**
T1110	Brute Force	Credential Access	**13.8%**
T1498	Network Denial of Service	Impact	**11.6%**
T0814	Denial of Service	Inhibit Response Function	**11.5%**

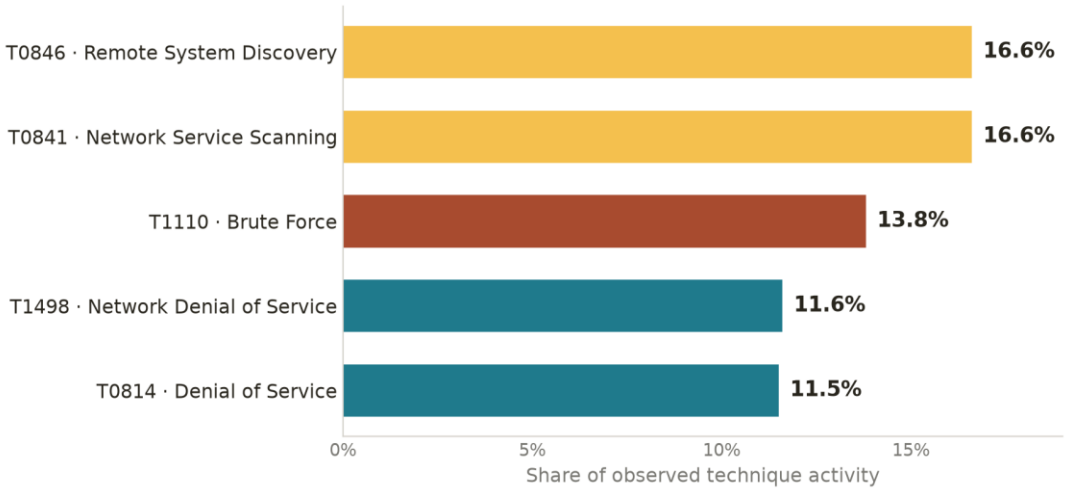

Figure 1. Top MITRE ATT&CK techniques observed in APAC manufacturing environments (Q1 2026).

Top threats affecting APAC manufacturing organizations

The most frequently observed MITRE ATT&CK techniques are concentrated across three major defensive themes: discovery activity, credential misuse, and service disruption. Together, the top five techniques account for

approximately 70% of observed activity, indicating that adversary behavior in the region is heavily weighted toward reconnaissance and availability-impacting actions.

Discovery techniques represent the largest share of the dataset. Remote System Discovery (T0846) and Network Service Scanning (T0841) account for roughly 33% together, making them the two most common techniques observed. This suggests that attackers are placing significant emphasis on identifying reachable assets, mapping network topology, and enumerating exposed services before attempting follow-on activity. In OT environments, this behavior is especially concerning because discovery can reveal critical controllers, engineering workstations, exposed management interfaces, and poorly segmented devices.

Credential Access is also prominent, with Brute Force (T1110) representing 13.8% of activity. This indicates continued attacker reliance on password guessing, credential stuffing, or automated login attempts against exposed services and accounts. The presence of brute-force activity alongside high levels of discovery suggests a common attack pattern: adversaries first identify accessible systems and services, then attempt to gain unauthorized access using weak, reused, or default credentials.

Impact-related behavior is another major finding, with various Denial-of-Service (DoS) activity combining to represent roughly 23% of the observed techniques. This highlights the operational risk posed by attacks that aim to degrade, interrupt, or prevent normal system functionality. In industrial environments, even temporary service disruption can affect visibility, process continuity, safety systems, or incident response capabilities.

Top Detected Malware Families and Threat Actors

Top categories of malware

Malware Category	Share
Miner	**50.3%**
Trojan	**42.8%**
Worm	2.95%
RAT	2.43%
Suspicious	1.51%

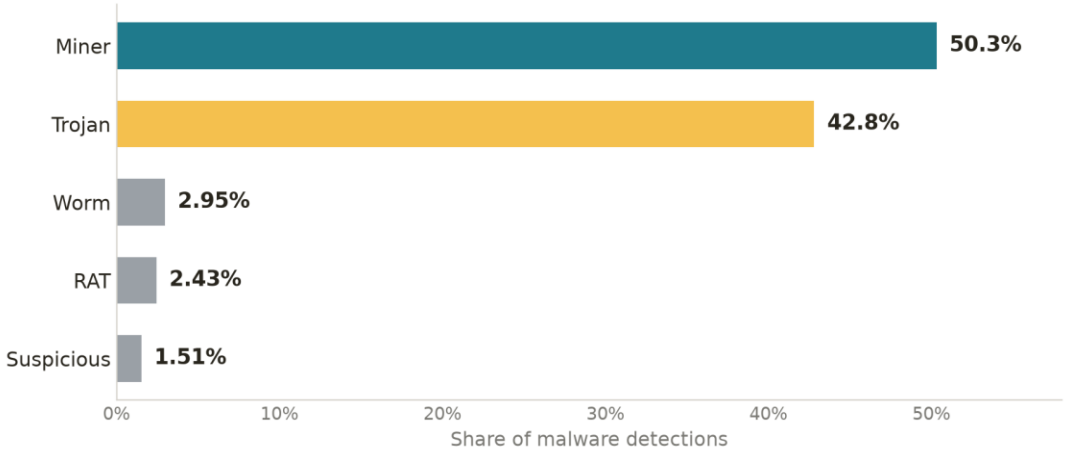

Figure 2. Categories of malware detected in APAC manufacturing environments (Q1 2026).

Miners represent the largest category by a clear margin, accounting for 50.3% of detections by performing unauthorized cryptocurrency mining or related resource-hijacking activity. While miners may not always be designed to directly disrupt industrial processes, they can still create operational risk by consuming CPU, memory, bandwidth, and power. In constrained OT and IoT environments, this added load can degrade performance, reduce device stability, and interfere with normal operations.

Trojans are the second-largest category, representing 42.8% of detections. This category is highly versatile, as trojans can be used at various attack stages — for example, to establish initial access, deliver additional payloads, steal information, or provide attackers with a foothold inside the environment.

Worms account for 2.95% of observed malware activity. Although this percentage is relatively small, worms remain important because of their ability to self-propagate across networks. In poorly segmented environments, worm activity can spread quickly between exposed devices, legacy systems, and unmanaged assets, creating a risk of rapid infection and operational disruption.

Remote Access Trojans (RATs) represent 2.43% of detections. While less common than miners and trojans, RATs pose a serious threat because they can give attackers interactive control over compromised systems. This capability can support surveillance, command execution, data collection, and further movement inside the network.

Finally, universal detections for various suspicious activity account for 1.51% of the dataset. This category likely reflects files, behaviors, or artifacts that do not cleanly map to a specific malware family or category but still warrant investigation. Even at a low percentage, suspicious detections can indicate emerging threats, incomplete classification, or early-stage activity that may later develop into a more clearly defined compromise.

Top malware families

Malware Family	Share
Generic	**62.5%**
DoublePulsar	**25.6%**
ANDROMEDA	6.04%
CobaltStrike	2.27%
Palevo	2.09%

The malware family distribution is highly concentrated, with Generic detections accounting for 62.5% of observed activity. This indicates that a large share of detections are associated with signatures, behavioral patterns, or artifacts that do not map cleanly to a specific named malware family. While this category is broad, its dominance suggests that many threats observed in OT and IoT environments may involve commodity malware variants, packed or modified samples, reused tooling, or activity detected by heuristic and generic rules rather than precise family attribution.

DoublePulsar represents the second-largest share at about a quarter of all detections, making it the most prominent named malware family in the dataset. Its high prevalence is notable because DoublePulsar has historically been associated with exploitation activity and post-exploitation access. In OT and IoT environments,

detections tied to this family may indicate exposed or unpatched systems, legacy Windows assets, or compromise attempts involving older but still effective attack infrastructure. The continued visibility of DoublePulsar-related activity reinforces the need for vulnerability management, patch prioritization, and monitoring for exploitation of known weaknesses across industrial networks.

ANDROMEDA accounts for 6.04% of detections. Although significantly smaller than Generic and DoublePulsar, its presence remains meaningful because ANDROMEDA has been widely associated with botnet activity, modular payload delivery, and broader criminal malware operations. In connected industrial and IoT environments, this type of activity can provide attackers with a foothold for additional malware deployment, credential theft, reconnaissance, or lateral movement.

Cobalt Strike represents 2.27% of detections. Even at a relatively low percentage, this family is important because Cobalt Strike is commonly associated with adversary simulation, red-team tooling, and malicious post-exploitation activity when abused by threat actors. Its presence may indicate more targeted or hands-on-keyboard activity compared with commodity malware and should generally be treated as a high-priority signal for investigation.

Palevo accounts for 2.09% of observed malware family detections. While less prevalent, Palevo is associated with worm-like propagation and botnet behavior, which can be especially problematic in environments with flat networks, unmanaged endpoints, or insufficient segmentation. Its presence highlights the continued relevance of older malware families that remain capable of spreading through exposed systems and weak security controls.

Top APTs targeting the region

Threat Actor	Associated Country	Share
Mustang Panda	China	**38.2%**
APT28	Russia	**25.2%**
APT39	Iran	8.13%
APT29	Russia	3.25%
APT41	China	3.25%

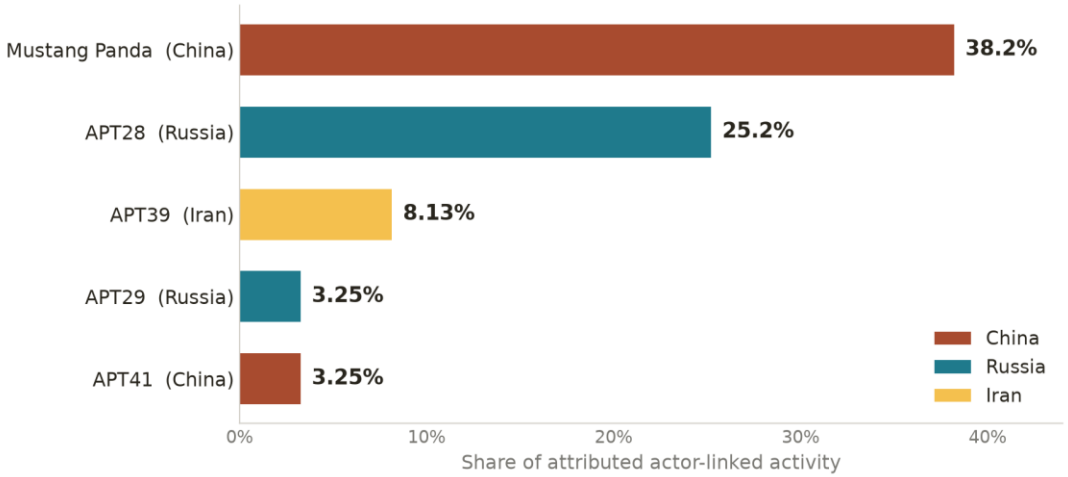

Figure 3. Top attributed threat actors and associated countries (Q1 2026).

The threat actor distribution shows a strong concentration of activity among a small number of state-associated or state-aligned groups. The top five actors account for approximately 78% of observed actor-linked activity, indicating that a relatively limited set of adversaries is responsible for the majority of attributed detections in the dataset.

China-associated activity represents the largest share of observed threat actor activity, driven primarily by Mustang Panda, which accounts for approximately 38% of observed activity, and supplemented by APT41 at 3.25%. Mustang Panda's prominence suggests sustained or repeated cyber-espionage activity, with likely emphasis on intelligence collection, persistence, and access to strategically valuable environments. Although APT41 appears at a much lower volume, it remains operationally significant because of its association with both espionage and financially motivated activity. Together, these actors highlight the need for OT and IoT defenders to monitor for stealthy intrusion patterns, phishing-driven access, command-and-control activity, suspicious use of legitimate tools or services, and lower-volume activity that may indicate more targeted, persistent, or high-impact campaigns.

Russia-associated activity represents a substantial share of the dataset, with APT28 accounting for about a quarter of observed activity and APT29 contributing a smaller but still significant portion. Together, these groups highlight persistent interest in espionage, long-term footholds, and operations against government, defense, infrastructure, and other strategically important organizations. In industrial and critical infrastructure contexts, this activity is particularly concerning because access to OT-adjacent systems, identity infrastructure, remote access services, or engineering environments can create pathways toward operational disruption, sensitive data collection, or sustained intelligence gathering.

Finally, APT39 accounts for 8.13% of activity and is associated with Iran. While its share is smaller than the leading China- and Russia-associated activity, it remains a meaningful presence in the dataset. This activity may reflect interest in intelligence gathering, monitoring of targeted organizations, or access to sectors with strategic or geopolitical relevance. For defenders, APT39-related activity should be treated as a signal to strengthen monitoring around identity systems, exposed services, and anomalous access patterns.

Top Recent Vulnerabilities in OT Assets

CVE ID	CVSS	Severity	Associated Assets
CVE-2025-40820	8.7	**HIGH**	Siemens Interniche IP-stack based industrial devices
CVE-2025-7353	9.3	**CRITICAL**	Rockwell Automation ControlLogix Ethernet Modules
CVE-2025-40833	8.7	**HIGH**	Siemens industrial networking devices
CVE-2025-0631	8.7	**HIGH**	Rockwell Automation PowerFlex 755 drives
CVE-2025-40943	9.4	**CRITICAL**	Siemens SIMATIC S7-1500

The telemetry data suggests that the most commonly detected vulnerabilities are concentrated across critical OT infrastructure components, affecting mainly Siemens and Rockwell Automation devices. This concentration is significant because the impacted asset types include systems that play central roles in industrial communication, control, and process operations, rather than only peripheral IT infrastructure. Affected devices include industrial controllers, communication modules, networking equipment, device communication components, and drive

systems, all of which can be essential to maintaining visibility, connectivity, and operational continuity in OT environments.

From a severity perspective, the dataset is split between HIGH- and CRITICAL-risk vulnerabilities, indicating that these findings should be treated as priority items for validation and remediation planning. The CRITICAL-risk vulnerabilities are associated with key control and communication assets, where exploitation could create opportunities for unauthorized access, disruption of industrial communications, or interference with operational processes. The HIGH-risk vulnerabilities affect supporting industrial networking, device communication, and drive systems, which may still have meaningful operational consequences if exploited — particularly in environments with limited segmentation, exposed management interfaces, legacy firmware, or weak access controls.

CVSS severity distribution: APAC vs. global

Looking at the distribution of CVSS scores for vulnerabilities detected in the region at the end of Q1, we observe the following picture.

Figure 1. CVSS Severity Distribution — APAC Manufacturing (end of Q1 2026)

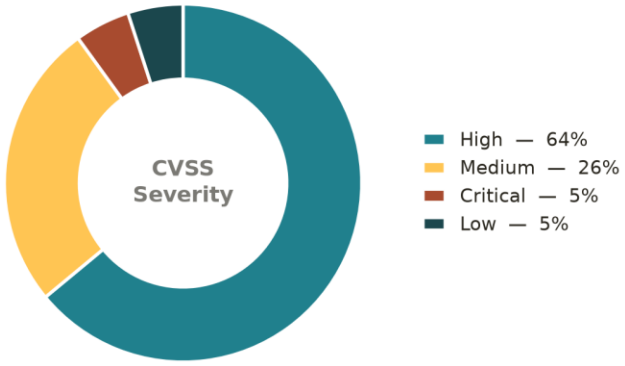

Figure 4. Distribution of CVSS score for vulnerabilities detected in APAC manufacturing organizations (end of Q1 2026).

As shown, vulnerabilities with a HIGH CVSS score constituted more than half of all detected CVEs, while CRITICAL ones accounted for 5%. Now, let us compare the situation with manufacturing companies globally.

Figure 2. CVSS Severity Distribution — Global Manufacturing (end of Q1 2026)

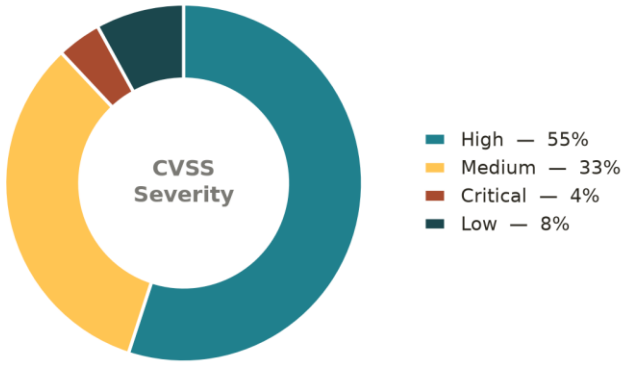

Figure 5. Distribution of CVSS score for vulnerabilities detected in manufacturing organizations globally (end of Q1 2026).

The data shows that the vulnerability situation appears significantly more severe in the APAC region when compared with the global Manufacturing baseline. In APAC, the proportion of vulnerabilities with a HIGH CVSS score is 9 percentage points above the average observed across Manufacturing environments worldwide. This gap suggests that organizations in the region may be facing a heavier concentration of serious vulnerabilities, increasing the likelihood that exposed or insufficiently protected assets could present meaningful operational risk. This regional difference is important because, depending on the affected asset, network placement, and availability of compensating controls, these vulnerabilities may support unauthorized access, disruption of industrial communications, lateral movement, or degradation of operational visibility. A higher share of HIGH-severity findings therefore points to a broader remediation burden and a greater need for disciplined vulnerability management across OT assets.

APAC Challenges

The APAC region presents a unique combination of risk factors, including rapid industrial digitization, high concentrations of manufacturing assets, and varying levels of cybersecurity maturity. The higher proportion of high-severity vulnerabilities suggests that organizations in the region may face more complex remediation challenges compared with global benchmarks.

Combined with sustained activity from state-associated threat actors, this environment calls for a proactive approach to threat detection, vulnerability management, and operational resilience. The convergence of discovery, credential access, and disruption techniques creates a multi-stage attack pattern that is difficult to defend against without strong coordination between IT and OT security teams.

Industrial environments often face unique constraints, including legacy systems, limited downtime tolerance, and incomplete visibility. These factors can delay detection and complicate response efforts. Additionally, attackers are increasingly targeting operational continuity: denial-of-service activity and malware-induced degradation may affect production processes, monitoring systems, and safety mechanisms, creating both financial and operational risk.

Conclusion

The data shows that adversaries are prioritizing techniques that help them discover targets, test access paths, and disrupt availability. For defenders, this reinforces the importance of continuous asset visibility, network traffic monitoring, segmentation, strong authentication controls, and early detection of scanning and brute-force behavior. Reducing exposed services, enforcing secure credential practices, and monitoring for unusual discovery patterns can help limit attacker options before activity progresses toward operational disruption.

Malware activity in APAC manufacturing environments is primarily driven by miners and trojans, with smaller but still meaningful contributions from worms, RATs, and suspicious artifacts. For defenders, this reinforces the need for strong endpoint and network-based detection, continuous asset monitoring, segmentation, secure configuration management, and rapid investigation of unusual resource consumption or unexpected outbound communications. Prioritizing detection of miners and trojans can address the majority of observed malware activity, while maintaining vigilance for lower-volume categories that may carry high operational impact.

Regarding vulnerabilities affecting OT environments, their distribution is driven by a combination of the devices prevalent in the region and local remediation practices, reinforcing the need to prioritize validation, mitigation planning, compensating controls, and monitoring for exploitation attempts across the affected environments. The average CVSS scores remain significantly higher in the APAC region compared with the global situation in the same sector. Where immediate remediation is not possible due to production constraints, compensating controls become especially important. These may include restricting access to vulnerable services, limiting exposure between IT and OT networks, strengthening remote access controls, and increasing detection coverage around affected systems.

Strategic Recommendations

Based on the observed trends, we advise manufacturing organizations to prioritize the following actions:

- Establish complete asset and network visibility across OT and IoT environments.
- Prioritize risk-based vulnerability management and remediation for OT environments.
- Strengthen detection capabilities for scanning, brute-force, and anomalous activity.
- Improve network segmentation and reduce the exposure of critical assets.
- Leverage AI-driven security systems to detect anomalies and threats.
- Strengthen malware prevention and detection in industrial networks.
- Detect and monitor wireless threats in OT and IoT environments.
- Enable intelligence sharing to improve collective cyber resilience.

These measures can greatly reduce the likelihood of successful attacks and improve the capacity to detect and respond to developing threats. The Q1 2026 threat landscape for APAC manufacturing underscores a consistent theme: attackers are exploiting visibility gaps to map environments, gain access, and interfere with operations. With discovery, credential access, and service disruption dominating activity, organizations must strengthen foundational security capabilities — including visibility, monitoring, and segmentation — to reduce risk. As threats evolve, a preemptive, intelligence-driven approach to OT security will be essential to protect critical manufacturing operations and ensure long-term resilience.

Put It Into Practice

One way to operationalize these recommendations is by leveraging specialized OT and IoT security platforms, such as Nozomi Networks. The Nozomi Networks platform helps organizations gain complete asset and network visibility, prioritize risks, detect threats, anomalies, and wireless attacks, and use threat intelligence to improve detection and response across industrial environments.

To learn more about the Nozomi Networks OT/IoT Security Platform and see it in action, request a demo today: **nozominetworks.com/demo**.

Related Content

- OT/IoT Cybersecurity Trends and Insights: 2025 2H Review — nozominetworks.com/ot-iot-cybersecurity-trends-insights-february-2026

Proposed byline: Nozomi Networks Labs — Manufacturing Threat Landscape, Q1 2026 APAC Edition.