DRONA
CYBER SOLUTIONS

// GLOBAL THREAT INTELLIGENCE BRIEF

Active Enterprise Compromise & Data Extortion Campaign Target Manufacturing Sector

In-depth technical analysis of unauthorized Active Directory takeover, 13.4 GB SQL database exfiltration, and threat actor 'BRKD' extortion operations.

PREPARED BY
Drona Cyber solutions Pvt Ltd

DATE OF ISSUE
August13,2026

CLASSIFICATION MATRIX
TLP : Amber

EXECUTIVE THREAT INTELLIGENCE ADVISORY

TARGET ENTITY	Namyang Industrial Co., Ltd.	**DATE OF ISSUE**	August 13, 2026
THREAT ACTOR	TA "BRKD"	**CLASSIFICATION**	TLP:AMBER
SECTOR / INDUSTRY	Automotive / Manufacturing	**RISK ASSESSMENT**	HIGH RISK
PRIMARY AD DOMAIN	`nyi.co.kr` / `nynexmo.com`	**EXTORTION DEMAND**	$400,000 USD (Barracuda)

EXECUTIVE SUMMARY

Drona Cyber Solutions Threat Intelligence Unit (TIU) has confirmed an ongoing critical breach and active extortion campaign targeting **Namyang Industrial Co., Ltd. (Namyang Nexmo)**, a premier South Korean automotive components manufacturer. The adversary, operating under the moniker **BRKD**, has exfiltrated over **13.4 GB of structured corporate data** containing 17,641,181 records across 800 database tables. Having failed to broker access on DarkForums, the threat actor has listed the victim on their newly established extortion site, **Barracuda**, demanding $400,000 USD under threat of public disclosure.

1. Incident Overview & Threat Landscape

Initial intelligence collection observed Threat Actor (TA) **BRKD** advertising elevated domain access and internal database backups belonging to Namyang Nexmo on *DarkForums*. The actor provided detailed proof of compromise confirming continuous `NT AUTHORITY\SYSTEM` level execution across multiple domain controllers and core database infrastructure.

Subsequent monitoring revealed that the initial access offering was withdrawn from forum sales, indicating a transition to direct data extortion or transfer to an affiliate. On August 12, 2026, the target entity was formally listed on the threat group's proprietary leak platform, **Barracuda**, with a countdown timer set at 2 days and 17 hours to enforce ransom compliance.

DarkForums Post

Figure 1: Initial Threat Actor Listing on DarkForums offering NT AUTHORITY\SYSTEM Domain Access.

2. Threat Actor Profile & NATO Admiralty Rating

TA **BRKD** established forum presence on July 21, 2026, quickly initiating multi-victim sales targeting enterprise infrastructure in manufacturing and healthcare across North America and Asia-Pacific regions.

Assessment Category	Rating Code	Analytical Evaluation
Source Reliability	**F - Cannot be judged**	Recent forum history provides insufficient baseline to establish long-term reliability.
Information Credibility	**3 - Possibly True**	Artifacts, schema screenshots, and SQL Database Mail configs match target infrastructure.
Extortion Platform	**Barracuda Leak Portal**	Dedicated onion portal utilizing countdown timers and public proof repositories.

3. Technical Forensic Analysis

3.1 Active Directory & Server Compromise

The threat actor maintained persistent interactive access utilizing a combination of remote interactive shells and **Remote Desktop Protocol (RDP)**. The scope of compromise includes:

- **Domain Environment:** `nyi.co.kr` Active Directory domain encompassing over 1,000 user accounts and 85 servers.
- **Elevated Rights:** System-level administrative privileges (`NT AUTHORITY\SYSTEM`) confirmed on a minimum of 4 central domain servers.
- **Database Administrative Access:** Full `sysadmin` rights on core Microsoft SQL Server 2012 clusters hosting QMS and MES databases.
- **Operational Discipline:** Threat actor activity ceased during standard Korea Standard Time (KST) working hours, demonstrating deliberate awareness of local SOC operations to evade active monitoring.

3.2 Exfiltration Scope & Data Repositories

The exfiltrated dataset consists of 13.4 GB of native Microsoft SQL Server backup files (`.BAK`), which were subsequently exported into structured CSV format. Analysis of sample schemas reveals exposure of high-value business operational data:

QMS Client Company Table

Figure 2: Recovered QMS Database (dbo.ClientCompany) revealing Client IDs, Business Numbers, and Contact Info.

- **Quality Management System (QMS):** Database containing 199 tables managing client company profiles (`dbo.ClientCompany`), approval lines, vehicle models, parts lists, and warranty claims.
- **Automated Mail System (sysmail):** Full dump of SQL Server Database Mail configuration (`dbo.sysmail_account`) showing system notification identity `system@nynexmo.com`.
- **Manufacturing Execution System (QMSI):** 19 operational tables containing part numbers, lot numbers (`LOT_NO`), inspection failure logs, and ERP supplier mappings (`dbo.TBL_IF_MES_OCCURRENCE_MEASURE`).

SQL System Mail Configuration

Figure 3: SQL Server Database Mail Account Configuration showing system sender identity.

QMSI MES Database

Figure 4: Manufacturing Execution System (QMSI) showing Lot Numbers and Production Measures.

3.3 File Staging & Forensic Timestamps

Forensic evaluation of filesystem artifacts indicates database backup operations occurred on July 29, 2026, followed by parsing and text extraction on July 30, 2026.

Database Backup Files

Figure 5: Database Backup (.BAK) files and subsequent exported text files in Windows directory.

4. Threat Actor Leak Site Listing

Following the initial forum post, the victim entity was formally published on the threat actor's extortion site "Barracuda" with a $400,000 USD ransom demand.

Barracuda Extortion Site

Figure 6: Extortion Listing on 'Barracuda' Leak Website with Countdown Timer ($400,000 Ransom).

5. MITRE ATT&CK Mapping

Tactic	Technique Name	ID	Observed Context
Initial Access	External Remote Services	`T1133`	Compromised RDP endpoints and VPN gateways.
Execution	Command & Scripting Interpreter	`T1059`	Execution of administrative PowerShell & batch scripts.
Lateral Movement	Remote Desktop Protocol	`T1021.001`	Internal RDP traversal across AD hosts.
Collection	Data from Repositories	`T1213`	Staging and extraction of native SQL `.BAK` databases.
Exfiltration	Exfiltration Over Web Service	`T1567.002`	Data upload via temporary web hosting (temp.sh).

6. Strategic Recommendations & Mitigation Roadmap

```
[CRITICAL ACTION PLAN FOR IT/SECURITY TEAMS]

1. IDENTITY ISOLATION: Force enterprise-wide password reset for all Active Directory users and service accounts in nyi.co.kr.
2. SESSION TERMINATION: Terminate all active RDP, VPN, and interactive shell sessions across the network immediately.
3. EDR DEPLOYMENT: Roll out centralized Enterprise Endpoint Detection & Response (EDR) to replacement basic Defender/AhnLab agents.
4. DATABASE HARDENING: Revoke sysadmin privileges from application accounts; encrypt all database backups (.BAK) at rest.
5. NETWORK SEGMENTATION: Isolate manufacturing network (MES) segments from corporate IT Active Directory domains.
```

DRONA
CYBER SOLUTIONS

Securing Today,
Empowering Tomorrow.

Drona Cyber Solutions

info@dronacybersolutions.com

+91 81609 68270

www.dronacybersolutions.com