Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

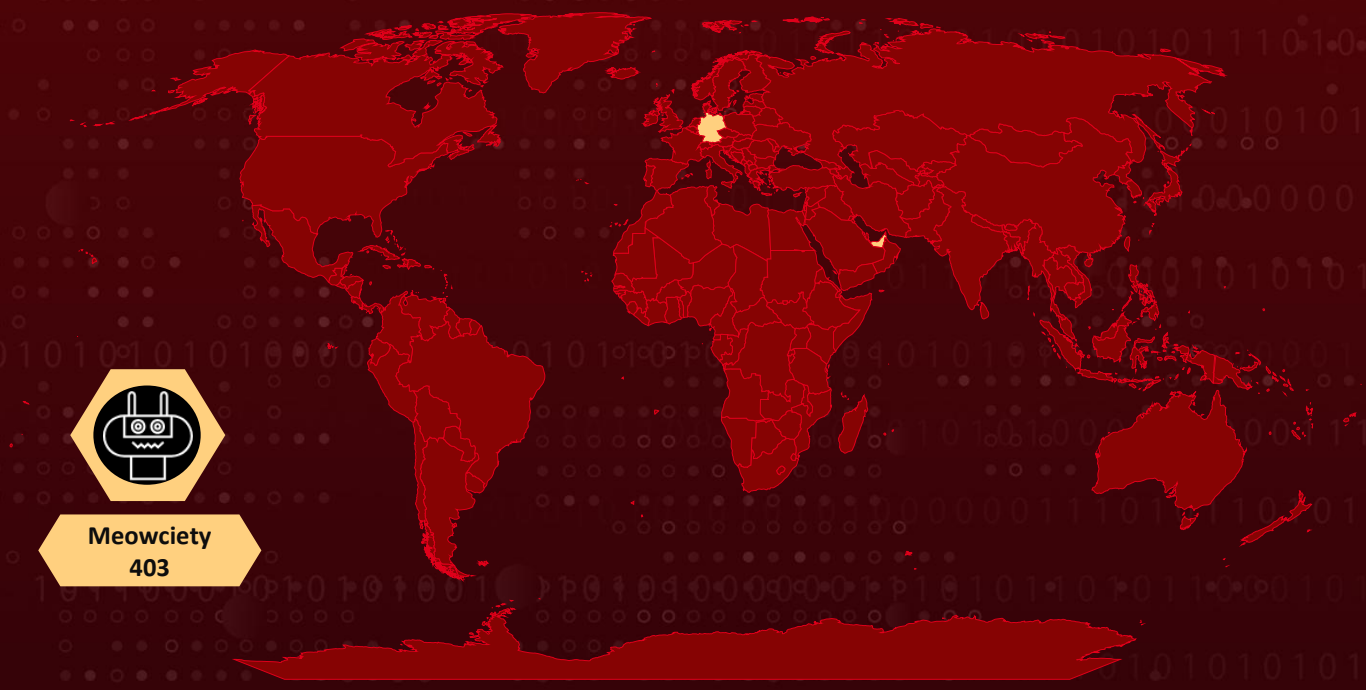
Paws on the Payroll: The Rise of Meowciety403

Date of Publication	Admiralty Code	TA Number
September 23, 2026	A1	TA2026278

Summary

First Seen: August 2026
Targeted Regions: United Arab Emirates, Singapore, Germany
Targeted Industries: Financial Services, Financial Brokerage and Foreign Exchange, Information Technology, IT Consulting, Technology
Threat Actor: Meowciety403 Ransomware Group (alias Nekoneko200)
Attack: Meowciety403, also tracked as Nekoneko200, is an emerging, financially motivated extortion group active since August 2026 that operates as a data broker rather than a confirmed encryption-based ransomware operation.

Attack Regions



Attack Details

#1

Meowciety403 is an emerging, financially motivated extortion group tracked since August 2026. It operates a dark web portal that serves as a leak site and is reachable at a single known Tor address, with Telegram channels under the handles monarodrigo and neko500 used for victim contact and public extortion pressure. Monetisation takes the form of data auctions, direct extortion, and double extortion, with ransom demands of USD 5,000 recorded against each of the Singapore victims.

#2

Data theft is the core of the business model and the best-evidenced stage of the operation. The group has claimed two to three victim disclosures: a financial brokerage and foreign exchange firm in the United Arab Emirates, from which it lists 216 PDF files of internal documentation, HR management records, daily corporate action reports, legal documents, and API keys; and three Singapore-based technology and consulting entities.

#3

It also lists over 5,400 candidate profiles, payment inventories, internal documents, SQL files, backend code structures, and bank account numbers with SWIFT codes. Its leak post for the UAE victim opens with the claim that operators had successfully infiltrated the target's systems. Based on the evidence, Meowciety403 appears to be a data broker rather than an encryption-based operation, so treat the encryption stage as unconfirmed pending further evidence.

Recommendations

Restrict and Monitor Remote Desktop Exposure: Remove direct internet exposure of RDP, place all remote access behind a VPN or zero-trust broker, enforce network-level authentication, and alert on RDP sessions that originate from workstations rather than administrative jump hosts.

Detect Bulk Data Staging and Egress: The group's claims centre on high-volume document, SQL, and source code theft. Deploy data loss prevention and network anomaly detection on file servers, code repositories, and HR and finance systems, and alert on unusual archive creation, large outbound transfers, and access to hundreds of documents by a single account in a short window.

Maintain Immutable, Offline Backups and Test Recovery: Although the encryption stage is unconfirmed. Keep immutable or air-gapped backup copies outside the production domain, protect volume shadow copies and backup catalogues from deletion, and rehearse restoration timelines against the systems this group targets.

Segment High-Value Business Systems: Brokerage, HR, payroll, and recruitment platforms are the datasets this group monetises. Place them in separate network segments with controlled east-west traffic, so that credential compromise on a general workstation does not grant a direct path to the records the group seeks.

Monitor for Third-Party and Shared-Founder Exposure: The Singapore victims were disclosed as a set of sites under common ownership, which indicates that shared infrastructure or shared administration can widen a single compromise. Assess vendors, sister companies, and shared hosting or administrative accounts for reused credentials and common management planes.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1547: Boot or Logon Autostart Execution	
Defense Evasion	T1562: Impair Defenses	
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
	T1080: Taint Shared Content	
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
TOR Address	hqhx32msbc545v233d55cvjedj5rqnv55bvzkavjv2q46qwuuannc4id[.]onion
URLs	hxxp[:]//hqhx32msbc545v233d55cvjedj5rqnv55bvzkavjv2q46qwuuannc4id[.]onion/, hxxps[:]//t[.]me/monarodrigo, hxxps[:]//t[.]me/neko500
Telegram Handle	monarodrigo, neko500

Recent Breaches

https://century.ae
https://demand.sg
https://marginwheeler.com
https://swiftly.sg

References

https://socradar.io/free-tools/ransomware-intelligence/groups/meowciety403

https://socradar.io/free-tools/ransomware-intelligence/victims/we-have-successfully-infiltrated-your-systems-meowciety403-ed3a0b40?_v=1789794975499&_chunk_retry=1

https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/meowciety403

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 23, 2026 • 6:00 AM

More at www.hivepro.com