ADVISORY FOR ICM SECTOR

TRAVELING SPIDER Targets VPN Appliances with INC Ransomware

Original report published on: May 07, 2026

Executive Summary

The TRAVELING SPIDER group offers ransomware-as-a-service (RaaS), and an affiliate likely conducted at least five intrusions between February 2026 and April 2026, gaining initial access through internet-exposed FortiGate VPN appliances before deploying INC ransomware across VMware ESXi and Windows systems.

Across multiple incidents, the affiliate consistently used Rclone[i] to exfiltrate data to Wasabi S3[ii] buckets and deployed PowerShell scripts for Active Directory reconnaissance. Several of these scripts exhibited characteristics commonly associated with AI-generated code, including structured formatting and verbose documentation patterns.

The affiliate is assessed as likely to continue targeting organisations with internet-exposed FortiGate VPN appliances for initial access in the near term and to employ similar post-compromise techniques including data exfiltration via Rclone and deployment of INC ransomware.

Background

Following initial access through FortiGate VPN appliances, the affiliate conducted lateral movement primarily using Remote Desktop Protocol (RDP), with additional remote execution performed via Windows Remote Management (WinRM). Network discovery activities included the use of Advanced IP Scanner to identify reachable systems and potential targets for lateral movement.

Credential and system manipulation activities were observed in multiple incidents. This included adding accounts to domain administrator groups and executing system-level commands such as *takeown* and *icacls* to modify file ownership and permissions across entire drive volumes. In some cases, registry modifications were also performed to enable Restricted Admin mode for RDP, facilitating credential theft and lateral movement.

Active Directory reconnaissance was conducted using PowerShell to enumerate domain computers and map network shares and storage locations. Multiple versions of custom reconnaissance scripts were observed, suggesting iterative development over the course of the attack.

Data exfiltration was consistently performed using Rclone, with stolen data transferred to Wasabi S3 buckets named after the victim organisations. Targeted data sets included Office documents, email files, CAD files, and other business-critical data. Across the observed incidents, the affiliate deployed INC ransomware on VMware ESXi hypervisors and/or Windows systems.

Detection and Mitigation

IMDA recommends that organisations perform continual testing and validation of existing security controls to ensure effective detection and prevention of the TRAVELING SPIDER activities described in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).

- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
    - Create, test and validate detection rules against the threat behaviours.
    - Review and restrict unnecessary processes, ports, and protocols based on business requirements.
- Monitor for the following activities and implement corresponding detection rules:
    - Rclone execution, particularly when transferring data to external cloud storage services or exhibiting bulk data transfer behaviour.
    - Anomalous PowerShell execution involving Active Directory enumeration and network share discovery.
    - Execution of network reconnaissance tools, including Advanced IP Scanner.
    - Unusual use of remote administration protocols, including RDP and WinRM.
- Ensure all VPN appliances are promptly patched and updated.
- Minimise internet exposure of VPN appliances where possible and review firewall rules to restrict access to only authorised sources.
- Require VPN connections to originate only from trusted, corporate-managed devices using device certificate-based authentication where feasible.
- Implement network segmentation to isolate backup and recovery infrastructure from production environments.
- Restrict administrative access to backup systems and critical infrastructure components.
- Maintain a 3-2-1 backup strategy by keeping at least three (3) copies of critical data on two (2) different storage media, with one (1) copy stored offline or offsite. Regularly test backup restoration procedures to ensure data can be successfully recovered in the event of a ransomware incident.
- Enforce multi-factor authentication (MFA) for all VPN access.
- Regularly audit VPN user accounts and remove inactive accounts and credentials belonging to former employees and contractors.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

IP Addresses	Description
185.254.97[.]249	IP addresses used by threat actor
185.174.100[.]201	
193.169.245[.]116	
186.65.113[.]111	

Hostname	Description
DESKTOP-2MN0M9R	Hostname used by threat actor

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1133	External Remote Services
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Privilege Escalation	T1098	Account Manipulation
Defense Evasion	T1222.001	File and Directory Permissions Modification
	T1556	Modify Authentication Process
Credential Access	T1555.005	Credentials from Password Stores
Discovery	T1087.002	Account Discovery: Domain Account
	T1135	Network Share Discovery
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol
	T1021.006	Remote Services: Windows Remote Management
Collection	T1119	Automated Collection
Exfiltration	T1567.002	Exfiltration Over Web Service
Impact	T1486	Data Encrypted for Impact

[i] Rclone is an open-source command-line tool that synchronizes, copies, and manages files between local systems and cloud or remote storage services.

[ii] Wasabi S3 is an Amazon S3-compatible cloud object storage service by Wasabi Technologies that provides low-cost storage for backups, archives, and application data.