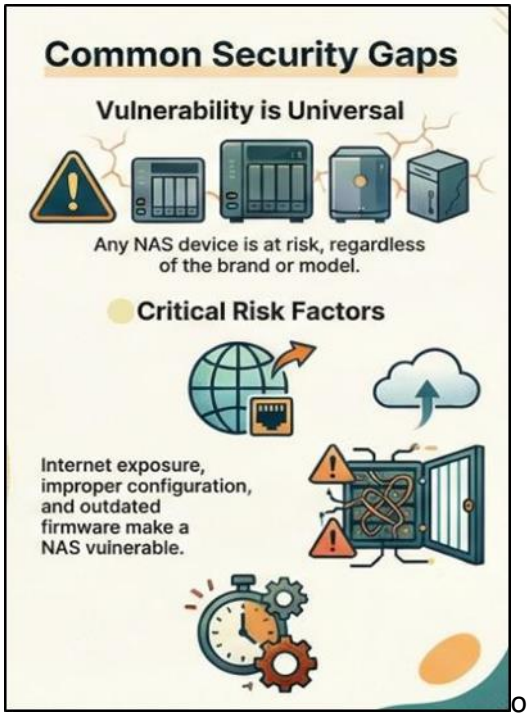
ADVISORY

Ransomware Groups Targeting NAS Devices used by CA and Consulting Firms

Executive Summary: Indian Cyber Crime Coordination Centre (I4C) has observed a surge in ransomware incidents targeting Chartered Accountancy (CA) firms and consulting organizations in India, as reported on the National Cyber Crime Reporting Portal (NCRP). Threat analysis indicates that ransomware groups are conducting targeted cyber-attacks against Network Attached Storage (NAS) devices, leading to complete encryption of organizational data, data theft, and extortion threats.

NETWORK ATTACHED STORAGE (NAS): OVERVIEW & RISK

Network Attached Storage (NAS): Network Attached Storage (NAS) is a dedicated file storage device connected to organization's network that provides centralized data access to multiple users and client devices. It functions like a private, on-premises cloud for storing and sharing critical business data.



o

Why NAS Devices Are Prime Targets

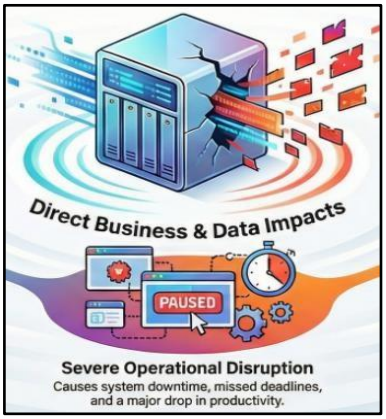
A compromised NAS can lead to total loss of both primary data and backups, making recovery extremely difficult. For this reason, ransomware groups actively and systematically target NAS devices. Any NAS that is internet-exposed, misconfigured, or running outdated firmware is vulnerable regardless of the vendor or model.

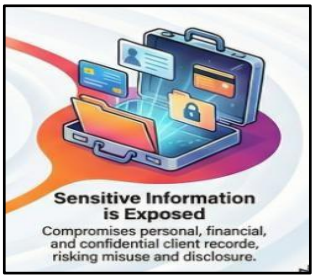
MODUS OPERANDI

- **Reconnaissance:** Automated scanning identifies internet exposed NAS management interfaces
- **Initial Access:** Exploitation of unpatched vulnerabilities, weak credentials, or missing MFA
- **Data Theft:** Exfiltration of sensitive client data before encryption
- **Encryption:** Deployment of ransomware across all volumes and backups
- **Double Extortion:** Ransom demand with threats to publicly release stolen data

POTENTIAL IMPACTS

- **Loss of Critical Business Data:** Complete loss of essential business data, including financial records, client information, and operational files stored on NAS systems.
- **Operational Disruption:** Severe disruption of business operations and client services, resulting in system downtime, missed deadlines, and reduced productivity.
- **Exposure of Sensitive and Regulated Information:** Compromise of personal data, financial data, and confidential client records, increasing the risk of data misuse and unauthorized disclosure of the information.
- **Financial Loss and Reputational Damage:** Significant financial losses arising from ransom demands, recovery and remediation costs, prolonged business interruption.
- **Legal and Regulatory Implications:** Mandatory breach reporting, regulatory non-compliance, potential penalties, and exposure to legal action.





NAS SECURITY RECOMMENDATIONS

1. **Safeguard Internet Exposure**
    - Access to NAS may be restricted to limited set of IP or network; to reduce attack surface.
    - Multi-Factor authentication may be introduced.
2. **Emergency Security Updates**
    - Default passwords may be changed.
    - Apply all available firmware and security patches
    - Disable unused accounts, services and legacy protocols (FTP, Telnet, SMBv1)
3. **Backup Protection**
    - Implement offline, air-gapped backups (physically disconnected)
    - Use immutable backup solutions (cannot be encrypted or deleted)
    - Test restoration procedures monthly
4. **Monitoring & Detection**
    - Enable comprehensive logging on NAS, firewalls, and authentication systems
    - Configure alerts for failed logins, unusual access, and large data transfers
5. **Incident Response**
    - Maintain forensic expert and legal counsel contacts
    - Isolate affected systems immediately (do NOT power off)
    - Report any cybercrime incidents on https://cybercrime.gov.in or call at 1930

VENDOR SECURITY ADVISIORIES:

SOLUTION: Ensure timely implementation of security updates as per vendor advisories.

QNAP: https://www.qnap.com/en/security-advisory

Synology: https://www.synology.com/security/advisory

Follow I4C's Social Media handles - CyberDost on

Source: *Indian Cybercrime Coordination Centre (I4C)*