AI ANALYSIS AND SUMMARY

CRITICAL SECURITY ALERT

This report contains a comprehensive analysis of compromised credentials associated with **nare.com** for the user **admin@nare.com** . Our security assessment has identified potentially compromised accounts that require immediate attention.

Breached User Details

User Name: admin@nare.com

User: admin@nare.com

Breached Date: 2024-12-03

Compromised Passwords: • FASS@098

URLs: • https://fas.nare.com

CONFIDENTIAL INFORMATION

This document contains sensitive security information. Distribute only to authorized personnel and handle according to your organization's data security policies.

Incident Report: Data Breach and Credential Compromise

Report Generated Date: September 2, 2025

1. Overview of the Incident

This report details a serious security incident involving a data breach that resulted in the compromise of user credentials.

On **Tuesday, December 3, 2024, at 21:13:41 UTC**, a device associated with the user admin@nare.com was infected with malicious software (malware). This malware successfully stole the password FASS@098 for the admin@nare.com account, along with other sensitive information from the infected device.

The compromise means that an unauthorized party now possesses this password and potentially has access to the user's accounts, both personal and organizational, that use this or similar credentials.

2. Compromised Device Information

The following key technical details were identified from the compromised device:

- **Operating System:** Windows 11 Pro (64-bit)
- **Computer Name:** DESKTOP-D1TDGT8
- **User Account (on device):** Z
- **Antivirus Software:** Windows Defender
- **RAM Size:** 32 GB
- **Processor (CPU):** Intel(R) Core(TM) i5-7300HQ CPU @ 2.50GHz
- **Graphics Processor (GPU):** Intel(R) HD Graphics 630
- **Display Resolution:** 1920x1080
- **IP Address:** 52.62.97.114
- **Country of Origin:** United States
- **Date/Time of Malware Activity (Local Device Time):** August 27, 2024, 11:08:00 PM (UTC-4)
- **Operating System Install Date:** March 17, 2024, 02:18:19 AM
- **Malware Location on Device:** C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe

3. Severity & Potential Impact

This incident is **severe** due to the direct theft of a password, especially for an account with an admin.com domain, which implies potential administrative access or privileged organizational roles.

- **For the User (admin@nare.com):**

  •Identity Theft: The stolen password and device information could be used to impersonate the user online.**•Financial Fraud:** If the same password or similar credentials are used for banking, shopping, or other financial services, these accounts are at high risk of unauthorized access and financial loss.**•Account Takeover:** Personal email, social media, and other online accounts could be accessed by the attacker.
- **For the Organization (if nare.com is an organizational domain):**

  •Unauthorized Access: The stolen password could grant an attacker access to internal systems, databases, or sensitive company data, leading to further breaches.**•Data Loss/Manipulation:** Attackers could steal, alter, or delete critical organizational data.**•Reputational Damage:** A breach involving an administrative account could severely damage the organization's reputation and trust with clients and partners.**•Further Malware Spread:** If the compromised device or account is used within the organizational network, it could facilitate the spread of malware to other systems.

4. Immediate Actions

To mitigate further damage, the following actions must be taken immediately:

- **Change Password:** Immediately change the password for admin@nare.com. Create a new, strong, and unique password that has not been used before.
- **Isolate Device:** Disconnect the compromised device (DESKTOP-D1TDGT8) from all networks (Wi-Fi, Ethernet) to prevent further spread of malware or data exfiltration.
- **Scan for Malware:** Conduct a full, comprehensive scan of the isolated device using reputable antivirus software to identify and remove any remaining threats.

- **Notify IT/Security Department:** Report this incident immediately to your organization's IT or Security department for further investigation and containment.

5. Security Recommendations

To enhance security and prevent future incidents:

- **Password Management:**

  •Change All Passwords: Change passwords for *all* other online accounts where FASS@098 or any similar password might have been used. Use a unique, strong password for each account.**•Password Manager:** Consider using a reputable password manager to generate and securely store unique, complex passwords for all your accounts.
- **Multi-Factor Authentication (MFA):**

  •Enable MFA Everywhere: Activate Multi-Factor Authentication (MFA) on all accounts that support it (email, banking, social media, work accounts). This adds an extra layer of security, making it much harder for attackers to access your accounts even if they have your password.
- **Account Monitoring:**

  •Financial Accounts: Regularly monitor bank statements, credit card activity, and other financial accounts for any suspicious or unauthorized transactions.**•Email & Online Accounts:** Review login history and activity logs for all critical online accounts for any unfamiliar access attempts.
- **Device Security:**

  •Operating System Reinstallation: For the compromised device, a complete reinstallation of the operating system (a "clean wipe") is strongly recommended to ensure all traces of malware are removed.**•Software Updates:** Keep your operating system, web browsers, and all software up-to-date with the latest security patches.**•Antivirus Software:** Ensure robust and regularly updated antivirus software is installed and actively scanning on all your devices.
- **Security Awareness:**

  •Phishing Awareness: Be extremely cautious of suspicious emails, messages, or links. Do not click on attachments or links from unknown senders.**•Organizational Training:** Participate in any security awareness training provided by your organization.

By taking these steps, we can significantly reduce the risk of future compromises and protect sensitive information.

Copyright © 2025 Vigile AI, Inc.
1600 Bryant St #411447 San Francisco | CA 94141 | support@vigile.ai