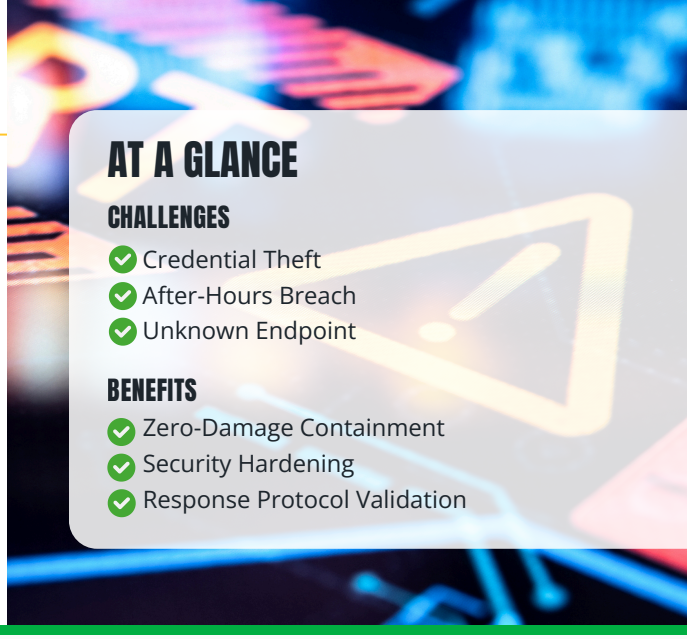
Net Friends

CASE STUDY

Net Friends Stops an After Hours Breach

A recent Saturday night saw an urgent NetSafe MDR alert. An unknown endpoint was accessing Server AB via the VPN using stolen credentials.



AT A GLANCE

CHALLENGES

- Credential Theft
- After-Hours Breach
- Unknown Endpoint

BENEFITS

- Zero-Damage Containment
- Security Hardening
- Response Protocol Validation

PROBLEM

An employee's account was compromised, triggering a NetSafe® MDR alert for activity from an unknown endpoint. The attacker was actively using the VPN to access the client's internal server.

APPROACH

Incident Identified: The team immediately confirmed an active security incident.

Containment: To halt the threat, Server AB was immediately isolated from the rest of the network systems. The compromised employee account was immediately locked out.

Investigation: Comprehensive system scans were then initiated to determine the full extent of the compromise, specifically looking for indicators like backdoors, newly created administrator accounts, or malicious software.

Security Remediation: Once the systems were confirmed clean and the threat mitigated, the employee's account password was changed, and Server AB was safely returned to the network.

SOLUTIONS

Following a NetSafe MDR report, Net Friends IT Experts promptly initiated the standardized response playbook. Compromised accounts were immediately disabled, and targeted servers were isolated to contain the threat. Comprehensive system scans verified the complete removal of all malicious accounts and software. Once the threat was fully neutralized, services were safely restored by re-enabling access and removing affected servers from isolation.

RESULTS

The Net Friends on-call team immediately executed the standard incident response playbook, rapidly containing the breach by disabling the account and isolating the server before major damage could occur.

The Monday debrief confirmed the successful containment but highlighted the difficulty in tracing the root cause without an obvious phishing attempt, emphasizing the critical need for users to report suspicious links or emails.

To prevent future incidents, the team recommended a series of security enhancements: implementing MFA, disabling the public VPN login page, auditing service accounts, enforcing a lockout policy, and migrating the on-prem server to SharePoint. This quick response became the catalyst for a crucial security upgrade.

Net Friends

919-680-3763

NetFriends.com

Durham, North Carolina