Title: Potential Kerberoasting Activity - DataHaven Solutions
Date: 2025-10-26
Alert Type/Category: Privilege Escalation — Potential Kerberoasting Activity
Severity: Medium
Analyst Name:
Case #: INC-20251026-1901

DETECTION AND ANALYSIS

Alert Summary:

The Multi-source Correlation Engine detected potential Kerberoasting activity on DC-01.datahaven.local originating from WS-072.datahaven.local by user DATAHAVEN\kristin.hansen. Kerberoasting is a technique where an attacker requests Kerberos service tickets (TGS) for service accounts and then attempts to crack the ticket offline to obtain the service account password for privilege escalation and lateral movement [1]. Within 14 seconds, three successful 4769 TGS requests using the legacy RC4-HMAC encryption (0x17) were observed for distinct SPNs (MSSQLSvc/sql01.datahaven.local:1433, ldap/exchange01.datahaven.local, HTTP/intranet.datahaven.local) from 10.2.14.57 by DATAHAVEN\kristin.hansen; shortly after, a 4768 TGT request for DATAHAVEN\svc_sql was recorded and a successful logon to sql01.datahaven.local by DATAHAVEN\svc_sql was observed, indicating likely credential compromise and use of the service account. We recommend that you investigate this activity further, as the activity appears to have resulted in successful use of DATAHAVEN\svc_sql.

References:

1 - https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/kerberoasting/

Key Details:

User: DATAHAVEN\kristin.hansen
Host: WS-072.datahaven.local
Source IP: 10.2.14.57
Domain Controller: DC-01.datahaven.local
Domain: DATAHAVEN
Event IDs: 4769 (3), 4768 (1)
Authentication Package: Kerberos
Status: SUCCESS (all listed events)
Ticket Encryption Types:
- 0x17 (rc4-hmac) for TGS (4769)
- 0x12 (aes256-cts-hmac-sha1-96) for TGT (4768)

Service Accounts Targeted:
- DATAHAVEN\svc_sql
- DATAHAVEN\svc_exchange

- DATAHAVEN\svc_web
SPNs Observed:
- MSSQLSvc/sql01.datahaven.local:1433
- ldap/exchange01.datahaven.local
- HTTP/intranet.datahaven.local
Event Timeline:
- 2025-10-26T09:14:12+02:00 — 4769 TGS for MSSQLSvc/sql01.datahaven.local:1433 by DATAHAVEN\kristin.hansen using RC4-HMAC (SUCCESS)
- 2025-10-26T09:14:18+02:00 — 4769 TGS for ldap/exchange01.datahaven.local by DATAHAVEN\kristin.hansen using RC4-HMAC (SUCCESS)
- 2025-10-26T09:14:26+02:00 — 4769 TGS for HTTP/intranet.datahaven.local by DATAHAVEN\kristin.hansen using RC4-HMAC (SUCCESS)
- 2025-10-26T09:34:20+02:00 — 4768 TGT for DATAHAVEN\svc_sql from WS-072.datahaven.local using AES256 (SUCCESS)

Consequence:

If successful, the attacker can obtain service account passwords by cracking RC4-encrypted TGS tickets offline, enabling impersonation of targeted service accounts. This may allow unauthorized access to resources such as SQL databases, email, or web applications, facilitate lateral movement, and lead to further privilege escalation within the domain. The observed sequence suggests likely compromise and use of DATAHAVEN\svc_sql, which could expose sensitive data on sql01.datahaven.local and expand the attacker’s foothold.

CONTAINMENT

Executed Remediation Actions:

The following containment and eradication actions has been performed by our SOC:
- Isolated WS-072.datahaven.local via EDR network containment due to anomalous Kerberos TGS activity.
- Initiated a full EDR malware/IOC scan on WS-072.datahaven.local.
- Collected endpoint triage from WS-072 (running processes, active network connections, logged-on users, recent persistence points) for investigation and evidence preservation.

Recommended Remediation Actions:

Our SOC recommends that you do the following containment actions:
- Temporarily disable/lock the user account DATAHAVEN\kristin.hansen pending investigation.
- Reset passwords immediately for the targeted service accounts: DATAHAVEN\svc_sql, DATAHAVEN\svc_exchange, DATAHAVEN\svc_web; prefer rotation to strong random values or migration to gMSA where applicable.
- Invalidate existing Kerberos tickets for the above accounts and restart dependent services to force re-authentication.
- Disable RC4 for Kerberos tickets via Group Policy and enforce AES128/256 across the domain.

- Review domain controller and affected server logs (Event IDs 4768, 4769, 4624) around the noted times to validate any use of DATAHAVEN\svc_sql on sql01.datahaven.local and identify additional affected hosts.
- Consider forensic review and, if compromise indicators persist, reimage WS-072.datahaven.local from a known-good baseline before returning it to the network.