Potential Kerberoasting Activity Targeting Service Accounts in DataHaven AD 2025-10-26

Title: Potential Kerberoasting Activity Targeting Service Accounts in DataHaven AD
Date: 2025-10-26
Alert Type/Category: Privilege Escalation – Suspected Kerberoasting
Severity: Medium
Analyst Name:
Case #: INC-20251026-1901

DETECTION AND ANALYSIS

Alert Summary:

The Multi-source Correlation Engine detected potential Kerberoasting activity originating from workstation WS-072.datahaven.local (10.2.14.57) by domain user DATAHAVEN\kristin.hansen in the DataHaven environment. Kerberoasting is a credential-access technique in which an authenticated user requests Kerberos service tickets (TGS) for service accounts with SPNs and then performs offline brute-force attacks against the ticket ciphertext to recover high-privilege service account passwords for lateral movement and privilege escalation [1][2]. In this case, within a 14-second window the domain controller DC-01.datahaven.local logged three successful Kerberos service-ticket (4769) requests from WS-072.datahaven.local for distinct SPNs MSSQLSvc/sql01.datahaven.local:1433 (service account DATAHAVEN\svc_sql), ldap/exchange01.datahaven.local (DATAHAVEN\svc_exchange), and HTTP/intranet.datahaven.local (DATAHAVEN\svc_web), all using the weaker RC4-HMAC encryption type 0x17, followed later by a successful TGT (4768) request for DATAHAVEN\svc_sql with AES256 (0x12) and a successful logon (4624) to sql01.datahaven.local from the same source IP using the svc_sql account. This tightly grouped pattern of multi-SPN TGS requests from a user workstation, combined with subsequent successful use of the targeted SQL service account from that workstation, is strongly indicative of an adversary or tool on WS-072 leveraging the kristin.hansen account to harvest crackable TGS tickets for service accounts and then use a recovered svc_sql credential to access the SQL server, with a realistic risk of further lateral movement or data access under service-account privileges [3][4][5]. We recommend that you investigate this activity further, as the activity appears to represent an attempted Kerberoasting attack against multiple service accounts with potential compromise of DATAHAVEN\svc_sql.

References:

[1] MITRE ATT&CK – “Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)”, mitre.org.
[2] Picus Security – “What Is a Kerberoasting Attack?”, 2024.
[3] NCC Group – “Defending Your Directory: An Expert Guide to Combating Kerberoasting in Active Directory.”
[4] ManageEngine – “What is Kerberoasting”.
[5] TheHacker.recipes – “Kerberoast” technique overview.

Key Details:

Customer: DataHaven Solutions
Alert Name: Potential Kerberoasting Activity
Alert ID: ALRT-2025-10-26-KERBEROAST-DataHaven-001
Case ID: INC-20251026-1901
Category: Privilege Escalation (Kerberoasting)
Severity: Medium
Detected Time: 2025-10-26T09:34:27+02:00
Time Window: 2025-10-26T09:14:12+02:00 – 2025-10-26T09:34:27+02:00
User: DATAHAVEN\kristin.hansen
User Display Name: Kristin Hansen
Origin Host: WS-072.datahaven.local
Domain: DATAHAVEN / datahaven.no
Domain Controller: DC-01.datahaven.local
Target Host: sql01.datahaven.local
Source IP: 10.2.14.57
Authentication Package: Kerberos
Service Accounts Observed:
- DATAHAVEN\svc_sql
- DATAHAVEN\svc_exchange
- DATAHAVEN\svc_web
Target SPNs Observed:
- MSSQLSvc/sql01.datahaven.local:1433
- ldap/exchange01.datahaven.local
- HTTP/intranet.datahaven.local
Event IDs:
- 4769 (Kerberos Service Ticket Requested)
- 4768 (Kerberos Authentication Ticket Requested – TGT)
- 4624 (Successful Logon)
Ticket Encryption Types:
- 0x17 (rc4-hmac)
- 0x12 (aes256-cts-hmac-sha1-96)
TGS Request Count: 3 TGS requests for distinct SPNs within 14 seconds
IOC List:
- 10.2.14.57
- DC-01.datahaven.local
- WS-072.datahaven.local
- sql01.datahaven.local

Consequence:

The observed Kerberos activity indicates an attempt to obtain crackable service tickets for multiple service accounts that support SQL, Exchange and intranet services, which could enable an attacker to recover their plaintext passwords and impersonate these accounts. If the DATAHAVEN\svc_sql credential has been recovered, as suggested by the successful logon to sql01.datahaven.local from a user workstation, an adversary could access SQL databases and business data under service-account privileges, use this access for lateral movement and privilege escalation in Active Directory, and

potentially pivot further if other targeted service accounts (such as svc_exchange or svc_web) are also compromised. This may in turn allow broader compromise of mail, web, or application tiers and, depending on the privilege level of the affected service accounts, could ultimately lead to domain-level compromise and extensive data access or exfiltration.

CONTAINMENT

Executed Remediation Actions:

The following containment and eradication actions has been performed by our SOC:
- No actions applicable by the MDR SOC due to customer contract (EDR).

Recommended Remediation Actions:

Our SOC recommends that you do the following containment actions:
- Immediately investigate activity originating from WS-072.datahaven.local (10.2.14.57), and if malicious activity is confirmed, remove the host from the network and perform a full EDR/antivirus scan and forensic review before returning it to production.
- Temporarily disable or lock the user account DATAHAVEN\kristin.hansen until you have determined whether the account and associated workstation have been compromised.
- Reset the passwords for the service accounts DATAHAVEN\svc_sql, DATAHAVEN\svc_exchange and DATAHAVEN\svc_web to long, random values (or migrate them to gMSA where applicable), and ensure these accounts are not permitted to perform interactive logons from user workstations.
- Review sql01.datahaven.local for suspicious activity performed under DATAHAVEN\svc_sql (including Windows Security logs and SQL/application logs), and validate the integrity of critical databases hosted on this server.
- Reconfigure Kerberos settings to disable or restrict RC4-based ticket encryption for domain accounts and enforce AES-only encryption for Kerberos service tickets where possible.
- Enable or tune monitoring for Kerberos ticket events (4768, 4769) and successful logons (4624) involving these service accounts and workstation WS-072, and closely monitor for further anomalous TGS-request patterns or service-account logons from user endpoints.