Incident Report 2025-11-11

Title:
Date:
Alert Type/Category:
Severity: Low / Medium / High / Critical
Analyst Name:
Case #:

DETECTION AND ANALYSIS

Alert Summary:

We have observed Kerberos activity that indicates a sucessful kerberoasting attack in logs from DC-01.datahaven.local.

A kerberoasting attack leverages weak passwords and/or weak encryption algorithms by requesting a Kerberos Server Ticket for accounts that have Service Principal Names (SPNs) tied to them [1]. This allows the attacker to capture the Ticket Granting Service (TGS) ticket with the encrypted password and use it with password cracking tools.

In the observed activity the actor is seen sending Service Ticket requests from the user account DATAHAVEN\kristin.hansen for the following service accounts between 09:14:12 and 09:14:26:
- DATAHAVEN\svc_sql
- DATAHAVEN\svc_exchange
- DATAHAVEN\svc_web

The ticket encryption used in this environment appears to be the weak legacy method rc4-hmac. This method is weak to kerberoasting attacks and should not be used [2].

Approximately 20 minutes after the Service Ticket requests we observe a successful logon from the service account DATAHAVEN\svc_sql coming from the same IP as the Service Ticket requests. This could indicate that the password was cracked in the time between the Service Ticket request and the observed logon.

References

[1] https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/kerberoasting/
[2] https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/active-directory-hardening-series—part-4-%E2%80%93-enforcing-aes-for-kerberos/4114965

Key Details:

Source IP: 10.2.14.57
Source user: DATAHAVEN\kristin.hansen
Victim user: DATAHAVEN\svc_sql

Consequence:

This could indicate that both the user account DATAHAVEN\kristin.hansen and the service account DATAHAVEN\svc_sql have been compromised by an attacker.

CONTAINMENT

Executed Remediation Actions:

(if possible) - Isolated the host with IP 10.2.14.57

Recommended Remediation Actions:

- Investigate with the user if this is known activity
- Determine if this could indicate a compromise of the involved user accounts
- Determine if this could indicate a compromise of the involved host
- Disable the observed accounts and revoke active sessions
    - Identify the scope of the attack
    - When mitigated, initialize a password reset for the accounts
- Consider disabling weak encryption algorithms for Kerberos