# Permission Groups Discovery, Technique T1069 - Enterprise

Archived: 2026-04-05 15:33:45 UTC

**Sub-techniques (3)**

Adversaries may attempt to discover group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions.

Adversaries may attempt to discover group permission settings in many different ways. This data may provide the adversary with information about the compromised environment that can be used in follow-on activity and targeting.[1]

ⓘ

Platforms: Containers, IaaS, Identity Provider, Linux, Office Suite, SaaS, Windows, macOS

Contributors: Daniel Prizmant, Palo Alto Networks; Microsoft Threat Intelligence Center (MSTIC); Yuval Avrahami, Palo Alto Networks

Last Modified: 24 October 2025

## Procedure Examples

## Mitigations

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

## Detection Strategy

| ID | Name | Analytic ID | Analytic Description |
|---|---|---|---|
| DET0179 | Behavioral Detection of Permission Groups Discovery | AN0507 | Detection of adversary enumeration of domain or local group memberships via native tools such as net.exe, PowerShell, or WMI. This activity may precede lateral movement or privilege escalation. |
| | | AN0508 | Detection of group enumeration using commands like 'id', 'groups', or 'getent group', often followed by privilege |

| ID | Name | Analytic ID | Analytic Description |
|---|---|---|---|
| | | | escalation or SSH lateral movement. |
| | | AN0509 | Group membership checks via 'dscl', 'dscacheutil', or 'id', typically executed via terminal or automation scripts. |

## References


1. Red Team Labs. (2018, April 24). Hidden Administrative Accounts: BloodHound to the Rescue. Retrieved October 28, 2020.
2. Symantec Security Response. (2016, September 6). Buckeye cyberespionage group shifts gaze from US to Hong Kong. Retrieved September 26, 2016.
3. Nikita Rostovcev. (2022, August 18). APT41 World Tour 2021 on a tight schedule. Retrieved February 22, 2024.
4. GovCERT. (2016, May 23). Technical Report about the Espionage Case at RUAG. Retrieved November 7, 2018.
5. Ta, V., et al. (2022, August 8). FIN13: A Cybercriminal Threat Actor Focused on Mexico. Retrieved February 9, 2023.
6. Kessem, L., et al. (2017, November 13). New Banking Trojan IcedID Discovered by IBM X-Force Research. Retrieved July 14, 2020.
7. FireEye. (2018, March 16). Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries. Retrieved April 11, 2018.
8. Mandiant Incident Response. (2025, July 23). From Help Desk to Hypervisor: Defending Your VMware vSphere Estate from UNC3944. Retrieved October 13, 2025.
9. Yonathan Klijnsma. (2016, May 17). Mofang: A politically motivated information stealing adversary. Retrieved May 12, 2020.
10. Prizmant, D. (2021, June 7). Siloscape: First Known Malware Targeting Windows Containers to Compromise Cloud Environments. Retrieved June 9, 2021.
11. Cash, D. et al. (2020, December 14). Dark Halo Leverages SolarWinds Compromise to Breach Organizations. Retrieved December 29, 2020.
12. Frydrych, M. (2020, April 14). TA505 Continues to Infect Networks With SDBbot RAT. Retrieved May 29, 2020.
13. Hiroaki, H. and Lu, L. (2019, June 12). Shifting Tactics: Breaking Down TA505 Group’s Use of HTML, RATs and Other Techniques in Latest Campaigns. Retrieved May 29, 2020.
14. Dahan, A. et al. (2019, December 11). DROPPING ANCHOR: FROM A TRICKBOT INFECTION TO THE DISCOVERY OF THE ANCHOR MALWARE. Retrieved September 10, 2020.
15. CISA et al.. (2024, February 7). PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Retrieved May 15, 2024.

Source: https://attack.mitre.org/techniques/T1069