KNOWHOW APT Attack Report

Incident Overview

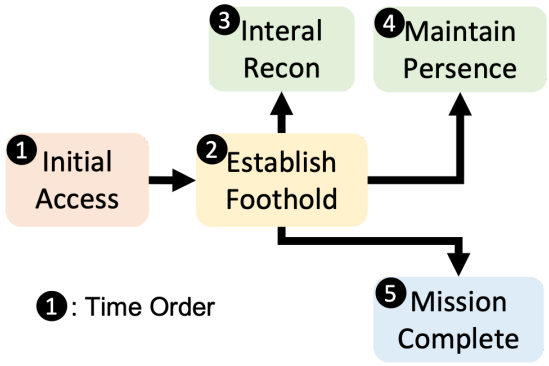
Date: 2024-05-09 **Reported By:** KNOWHOW
Incident ID: 00001

Executive Summary

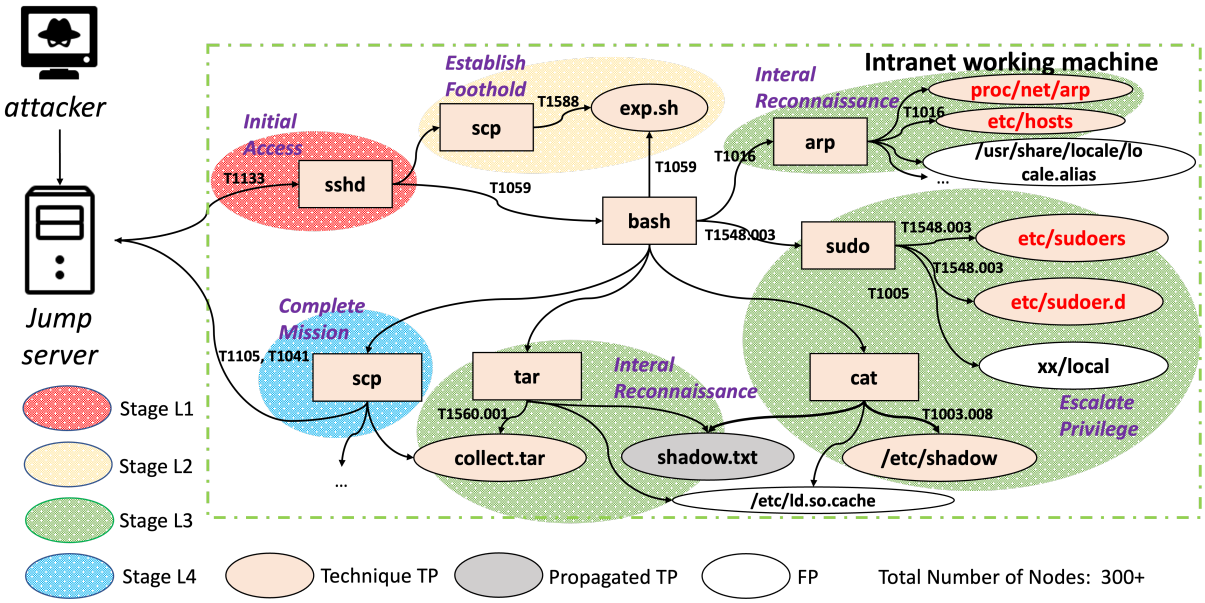
On 2024-05-09, KNOWHOW detected a sophisticated Advanced Persistent Threat (APT) attack originating from an external IP address (121.36.30.176). The attack exploited vulnerabilities in our internal network, specifically targeting critical infrastructure.

Attack Overview

1. **Attack Lifecycle Alert**



2. **Attack Provenance Graph**



Attack Details

1. **Initial Compromise**
    - **External IP:** 121.36.30.176
    - **Initial Access:** SSH connection to internal jump host (IP: 10.7.0.126) using sshd process.
2. **Lateral Movement**
    - After accessing the jump host, the attacker used the sshd process to pivot to an internal information processing machine (IP: 10.7.0.18).
3. **Establish Foothold**
    - Upon gaining access to the information processing machine, the attacker's bash process executed the following actions to establish foothold:
        - Created and wrote to `exp.sh` file using scp process.
        - Executed `bash ./exp.sh`, leading to the execution of commands to modify `sudoers` and `sudoer.d` files and read `/[pid]/local` files.
4. **Escalate Privilege**
    - The attacker used malicious scripts to achieve privilege escalation:
        - Executed `bash ./exp.sh`, leading to the execution of commands to modify `sudoers` and `sudoer.d` files and read `/[pid]/local` files, which allowed the attacker to gain access to sudo.
5. **Internal Reconnaissance**
    - After establishing a foothold, the attacker used arp, cat, tar commands to realize the internal reconnaissance and information collection of the victim's system:
        - Extracted `/etc/shadow` file content into `shadow.txt` using cat process.
        - Packaged `collect/shadow.txt` into `collect.tar` using tar process.
6. **Complete Mission** -The attacker transmited the critical information collected from the victim system to the external device to achieve the mission completion:
    - Transferred `collect.tar` back to 10.7.0.126 using scp process.

Indicators of Compromise (IOCs)

- **IP Addresses:**
    - External IP: 121.36.30.176
    - Internal Jump Host: 10.7.0.126
    - Internal Information Processing Machine: 10.7.0.18
- **Files Modified:**
    - `exp.sh`

- `/etc/sudoers`
- `/etc/sudoer.d`
- `shadow.txt`
- `collect.tar`

Historical Context and Related Incidents

This attack bears similarities to previous APT campaigns observed globally, such as attacks targeting critical infrastructure and utilizing SSH for initial access and lateral movement. Recent incidents in the cybersecurity community have highlighted similar tactics, techniques, and procedures (TTPs) used by threat actors to compromise networks for espionage purposes.

Mitigation Steps

1. **Immediate Actions**
    - Isolated affected systems from the network.
    - Changed credentials for compromised accounts.
    - Reviewed and updated firewall rules to limit external access.
2. **Long-term Recommendations**
    - Conducted thorough security audits and vulnerability assessments.
    - Enhanced monitoring and logging capabilities to detect similar intrusions in the future.
    - Implemented stricter access controls and multi-factor authentication mechanisms.

Conclusion

This incident demonstrates the persistence and sophistication of the attackers, highlighting the critical need for robust cybersecurity measures to protect against APT threats. Immediate remediation efforts have been undertaken, and ongoing monitoring will continue to safeguard our systems from future attacks.