Task 5 — Recent Malware Incidents: Methods & Mitigations

1. XZ Utils Backdoor — Supply-Chain Backdoor (CVE-2024-3094)
   When: March–April 2024
   What happened: Malicious code was slipped into XZ Utils 5.6.0/5.6.1, which could subvert sshd authentication paths on affected Linux builds—an OSS supply-chain compromise caught just before broad distro rollouts. (NVD, Red Hat Customer Portal, Red Hat)
   Attack method (kill chain):
   Poisoned upstream source tarballs → obfuscated build steps swap in a crafted object → modified liblzma intercepts used by OpenSSH on some builds, enabling remote auth bypass. (NVD)
   Mitigation / resolution:
   Immediate pin/downgrade to 5.4.x; revoke/replace affected packages; verify signatures, adopt reproducible builds, and tighten release vetting for critical OSS dependencies. (Red Hat, wiz.io)

2. Snowflake Customer Data Thefts — Credential-Based Intrusions (UNC5537)
   When: May–June 2024 (fallout and analysis continued into 2025)
   What happened: A financially motivated group ("UNC5537") accessed dozens of Snowflake customer instances (e.g., Ticketmaster, Santander) using stolen credentials, then exfiltrated and extorted large data sets. MFA gaps and contractor accounts were central in several cases. (Google Cloud, WIRED, Cloud Security Alliance)
   Attack method (kill chain):
   Infostealer-harvested creds (including contractor accounts) → login to internet-exposed Snowflake instances lacking MFA → database enumeration & mass exfiltration → extortion. (Google Cloud, WIRED)
   Mitigation / resolution:
   Mandate MFA/SSO for all users/service accts; rotate API keys; hunt for suspicious queries & network egress; review vendor/contractor access; follow joint guidance from Snowflake/Mandiant/CrowdStrike. (Daily Security Review)

3. ConnectWise ScreenConnect — Mass Exploitation to Ransomware (CVE-2024-1709/1708)
   When: February 2024 onward
   What happened: An auth-bypass flaw in ScreenConnect was weaponized at scale by ransomware crews (including Black Basta) to push payloads via remote-management infrastructure. (CISA)
   Attack method (kill chain):
   Internet-facing RMM appliance with auth bypass → hands-on-keyboard deployment of tools → lateral movement → ransomware execution across

managed fleets. (NVD)
Mitigation / resolution:
Patch to 23.9.8+ immediately; isolate RMM servers; rotate credentials/tokens; review logs for new users/sessions and post-exploitation tools. CISA placed CVE-2024-1709 on KEV due to active exploitation. (ConnectWise, CISA)

4. Palo Alto Networks PAN-OS GlobalProtect — Perimeter 0-Day Used in the Wild (CVE-2024-3400)
When: April 2024
What happened: A command-injection bug in GlobalProtect on certain PAN-OS versions allowed unauthenticated RCE on firewalls; exploitation in the wild was confirmed. (security.paloaltonetworks.com, CISA)
Attack method (kill chain):
Unauthenticated network access to GlobalProtect portal/gateway → command injection → root-level code execution on the firewall → potential pivoting and data access. (CISA)
Mitigation / resolution:
Apply fixed PAN-OS releases or vendor workarounds; restrict portal exposure; monitor configs and system logs for indicators; add firewall-level detections for suspicious command exec. (security.paloaltonetworks.com, CISA)

Key Takeaways & Defenses

- **MFA and identity hardening everywhere:** Snowflake intrusions again showed valid-cred logins are the easiest "0-day." Enforce MFA (incl. service & contractor accounts), conditional access, and rapid key rotation. (Google Cloud, WIRED)
- **RMM exposure = blast multiplier:** Patch or geofence tools like ScreenConnect; use allow-listing and separate admin identities; treat RMM like domain controllers for monitoring. (CISA)
- **Perimeter 0-days happen:** Keep appliances on dedicated patch cadence, reduce internet exposure, and deploy out-of-band logging so attackers can't blind defenses (PAN-OS case). (CISA)
- **Supply-chain scrutiny for OSS:** Verify signatures, prefer reproducible builds, monitor for anomalous build behaviors, and pin versions—XZ proved even "boring" libs can be weaponized. (Red Hat, NVD)

Prepared By: **vaishnav k**
Date: **Aug 17, 2025**