**Phase 1: Initial Access.** The attacker got inside Uber’s IT environment by gaining access to credentials to Uber’s VPN infrastructure.

**Phase 2: Discovery.** Most likely, this contractor did not have special or elevated privileges to sensitive resources but did have access to a network share, as did other Uber workers. This network share was either open or misconfigured to allow broad read ACL. Within the network share, the attacker discovered a PowerShell script containing hard-coded privileged credentials to Uber’s PAM solution.

A brief aside: Both IT teams and developers often automate tasks by creating scripts that need some form of credentials to perform authentication (e.g., manual backup or generating custom reports by pulling data from databases). These credentials could be anything from SSH keys and API tokens to other types of passwords and privileged tokens. To save time and help ensure automation, it’s common for developers to embed (or hard code) these credentials into the code. This leaves the credentials exposed to everyone with access to the code and makes them difficult to manage and rotate. In the Uber breach, hard-coded credentials granted administrative access to a privileged access management solution. These credentials appear not to have been rotated in some time — making them much easier to exploit.

**Phase 3: Privilege Escalation, Access PAM System.** By harvesting the hard-coded admin credentials for the privileged access management solution, the attacker was able to further escalate privileges.

**Phase 4: Access Secrets from PAM System, Reach Critical Company Systems.** According to Uber’s latest update, the attacker ultimately gained “elevated permissions to a number of tools.” By accessing secrets from the privileged access management solution, the potential for damage was significant: The attacker reportedly compromised access to the SSO and consoles as well as to the cloud management console where Uber stores sensitive customer and financial data.

**Phase 5: Data Exfiltration.** While Uber is still investigating the incident, the company confirmed that the attacker “downloaded some internal Slack messages, as well as accessed or downloaded information from an internal tool our finance team uses to manage some invoices.”