APT 32: Operation Cobalt Kitty
Victim Network Research & Plan

Host: VSphere

Key Victim Network Components

Workstations (2 Devices - Windows 10)

- Initial access to the network
- Spear-phishing victim
- Contained a link to install a fake flash player

Proxy Server (HA Proxy)

- Attackers were aware of the proxy server in the network
- Configured IPs and ports to still allow access to the external C&C network

Active Directory Server (Windows Server)

- Compromised the AD through pass-the-hash and pass-the-ticket

Web Server (centOS)

- Mock webserver for the company
- Could implement a database containing user information

Database Server (centOS)

- Contain desired files that will be extracted from the network

File Server (Windows Server)

- Network file share used to host target files

Firewall (vyOS)

- Main firewall used in network

Attacker Network Components

Attacker Workstation (Kali)

- Initiate attack (phishing)

C&C Server (Ubuntu)

- Contained payloads that victim network reached out to, once compromised

DNS Server

- Attackers used OpenDNS and Google's DNS server to mask the actual address of the C&C Server
- By using a known DNS server, it was less likely that the traffic would be filtered