APT37

AALIYAH CONNERS

Origin

- APt37 is a North Korean state-sponsored cyber espionage group.
- Active since at least 2012
- Also known: Inky Squid, Reaper, Redeyes
- Security research overlap/ Lazarus Group

Targets

- Their targets mainly consist of the countries:
- South Korea
- Japan
- Vietnam
- Russia
- China
- And parts of the middle east

Targets pt2

- Targets south Korean government agencies and organizations
- This group has targeted defense agencies working with national security
  - South Korea
  - U.S.
  - Cambodia

Techniques

- Spear Phishing emails: Attachments or links
- Credential Dumping: Uses tools to harvest credentials and then escalate privileges
- Abuse Elevation Control: Escalate privileges on comprised systems

Notable Attack

VeilShell Backdoor

Targeted Cambodian government officials, business executives and other high-profile targets with spear fishing.

The spearfishing attacks deployed malware such as the VeilShell backdoor. (a .zip archive containing a windows shortcut (.LNK file))

APT37 used social engineering tactics such as fake job offers and ‘critical’ emails to lure these people into clicking these links.

Motivation

- Espionage: Political data, military, economic objectives
- Destabilization: Disrupt critical infrastructure, defense systems