APT30

Overview

APT30 is a threat group suspected to be associated with the Chinese government. While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches.[1][2]

Tactics

Naikon and APT30's tactics focus on cyber espionage against governments and critical institutions in the Asia-Pacific region. They gain initial access through spear phishing emails, use zero-day and known vulnerabilities for remote code execution, steal sensitive geopolitically relevant intelligence, and maintain long-term control of target networks through persistence techniques

Techniques

Naikon and APT30 use spear phishing emails (T1566.001) to direct targets to web pages containing malicious attachments or links, exploit vulnerabilities for code execution (T1203), and transmit encrypted data through C&C servers (T1071.001) The malware used by Naikon communicates over the SSL protocol, and APT30's BACKSPACE and NETEAGLE backdoors use multi-level encryption and RC4 technology to protect data.

1. **Techniques Used:** Phishing: Spearphishing Attachment, User Execution: Malicious File
2. **Software used:** BACKSPACE, FLASHFLOOD, NETEAGLE, SHIPSHAPE, SPACESHIP

Procedures

Naikon sends emails with malicious attachments via spear phishing emails, which often contain known vulnerabilities such as CVE-2012-0158. When the target user opens the document, the malicious code installs a remote control tool and communicates with the C&C server, allowing the attacker to take control of the infected system through 48 different commands.APT30, on the other hand, primarily uses BACKSPACE and NETEAGLE backdoors in conjunction with DROP components, such as SHIPSHAPE and SPACESHIP, to target systems in isolated networks Perform infiltration. These malwares steal data from target systems over network or physical media and outbound data through encrypted C&C communications.APT30 further hides its activities through RC4 encryption and multi-level channels, and frequently updates its backdoor program to ensure persistent access control and data theft capabilities.