APT16

Overview

APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations.

Tactics

APT16's tactics focus on espionage, targeting political, media, and commercial organizations in Japan and Taiwan. They conduct Initial Access through spear phishing and utilize Privilege Escalation to take control of the system.APT16 also uses persistence and lateral movement tactics to maintain long-term access to the target environment.

Techniques

APT16 uses spear phishing emails with malicious attachments (T1566.001) to infiltrate and exploit software vulnerabilities to execute arbitrary code (T1203). They maintain persistence through backdoors and other malware (T1547) and outbound data through encrypted command and control (C2) communications (T1071.001). Elevation of privilege is achieved by exploiting software vulnerabilities (T1068).

1. **Techniques Used:** Compromise Infrastructure: Server
2. **Software used:** ELMER

Procedures

APT16 typically begins its attacks by sending spear phishing emails with malicious attachments. These emails contain malware or documents that exploit known vulnerabilities that are exploited for initial access. Once inside the system, APT16 deploys malware to establish a foothold, which in turn elevates privileges and maintains persistence in the environment. They use backdoors to communicate with command-and-control servers, often through encrypted channels to avoid detection.APT16 has repeatedly attacked organizations in Japan and Taiwan, focusing on collecting sensitive data and then outgoing the data through secure communication protocols. Their attacks are well-coordinated and designed for long-term espionage.