APT17

Overview

APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.

Tactics

APT17's tactics focus on cyber espionage, primarily targeting U.S. government and industry entities. They hide the origin of their command and control (C2) communications by acquiring infrastructure (T1583) and creating accounts on legitimate platforms (T1585). The goal is to blend in with normal network traffic, thereby making detection more difficult and maintaining long-term access.

Techniques

APT17 utilizes web services (T1583.006) such as Microsoft TechNet to host encoded C2 IP addresses and distributes legitimate content by creating legitimate accounts (T1585.002). The organization uses the BLACKCOFFEE malware to create reverse shells and perform file and process operations (T1059.003), whose communications are obfuscated through encoding.

1. **Techniques Used:** Acquire Infrastructure: Web Services, Establish Accounts
2. **Software used:** BLACKCOFFEE

Procedures

APT17 attack programs add an additional layer of obfuscation by embedding encoded C2 information in legitimate websites, such as Microsoft TechNet, rather than compromising them directly. They use legitimate user profiles to post encoded CNC data on forums and personal pages, which the BLACKCOFFEE malware decodes to locate actual C2 servers. This method, known as a “drop-dead resolver,” allows infected machines to query these legitimate websites for obfuscated IP addresses for further communication, making it more difficult for security researchers to detect. malware is able to create reverse shells, perform file operations, and execute new backdoor commands. This method allows APT17 to camouflage itself in network traffic and continuously spy while avoiding detection.