Night Dragon - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:38:35 UTC

Description(McAfee) Starting in November 2009, coordinated covert and targeted cyberattacks have been conducted against global oil, energy, and petrochemical companies. These attacks have involved social engineering, spear-phishing attacks, exploitation of Microsoft Windows operating systems vulnerabilities, Microsoft Active Directory compromises, and the use of remote administration tools (RATs) in targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations.

Attackers using several locations in China have leveraged C&C servers on purchased hosted services in the United States and compromised servers in the Netherlands to wage attacks against global oil, gas, and petrochemical companies, as well as individuals and executives in Kazakhstan, Taiwan, Greece, and the United States to acquire proprietary and highly confidential information. The primary operational technique used by the attackers comprised a variety of hacker tools, including privately developed and customized RAT tools that provided complete remote administration capabilities to the attacker. RATs provide functions similar to Citrix or Microsoft Windows Terminal Services, allowing a remote individual to completely control the affected system. To deploy these tools, attackers first compromised perimeter security controls, through SQL-injection exploits of extranet web servers, as well as targeted spear-phishing attacks of mobile worker laptops, and compromising corporate VPN accounts to penetrate the targeted company’s defensive architectures (DMZs and firewalls) and conduct reconnaissance of targeted companies’ networked computers.

Night Dragon may be related to APT 18, Dynamite Panda, Wekby.
