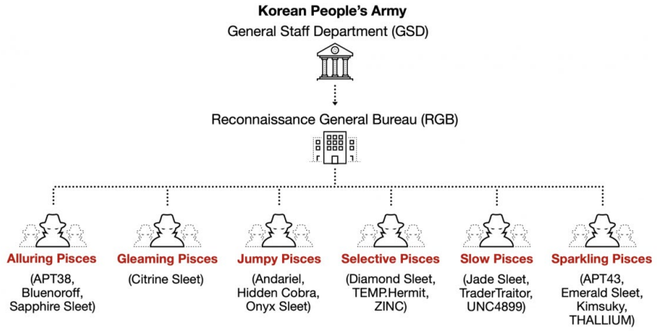
North Korean Advanced Persistent Threats (APTs)

This infographic provides an overview North Korean Advance Persistent Threats (APTs). North Korean APTs refer to a group of sophisticated cyber threat actors sponsored by the North Korean government. These APTs are known for their advanced techniques, persistence, and focus on achieving strategic objectives including espionage, sabotage, and financial gain. The primary goal of North Korean APTs is to support the country's national interests, which can involve stealing sensitive information, disrupting critical infrastructure, and generating revenue through cybercrime.

Democratic People's Republic of Korea (DPRK, also called North Korea)
Threat Actors under the Reconnaissance General Bureau



Notable North Korean APT Groups

Lazarus Group (APT38): Known for their involvement in high-profile attacks, including the 2014 Sony Pictures hack and the WannaCry ransomware outbreak in 2017.

Kimsuky (APT37): Focuses on cyber espionage, targeting South Korean and other foreign entities.

Andariel: A subgroup of the Lazarus Group, with a focus on stealing sensitive information and disrupting operations.

Reaper (APT37): Also known as StarCruft, is believed to be responsible for a range of cyber espionage activities.

Characteristics of North Korean APTs

State Sponsorship: North Korean APTs are believed to be directly sponsored by the North Korean government, with their activities closely aligned with the country's strategic objectives.

Advanced Techniques: These groups employ sophisticated techniques, including zero-day exploits, custom malware, and social engineering tactics, to infiltrate and persist within target networks.

Persistence: APTs are characterized by their ability to remain hidden within a network for extended periods, continuously gathering intelligence or waiting for the optimal moment to strike.

Diversified Targets: North Korean APTs target a wide range of sectors, including government agencies, defense industries, financial institutions, and technology companies, in various countries around the world.

Financial Motivation: In addition to espionage, North Korean APTs are motivated by financial gain, engaging in activities such as cryptocurrency theft, ransomware attacks, and online bank heists.

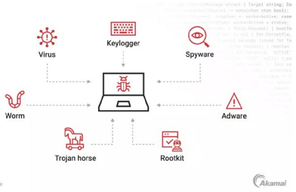
TTPs (Tactics, Techniques, and Procedures)

Spear Phishing:

Social Engineering:

Exploitation of Vulnerabilities

Lateral Movement:



Malware:

(Click picture for more info on TTP)

To combat North Korean Advanced Persistent Threats (APTs), organizations should keep software updated, use antivirus solutions, and implement intrusion detection systems. Regular security audits and personnel training on phishing are essential. Leveraging threat intelligence will help anticipate evolving tactics, enhancing overall security.

Source: Threat Assessment: North Korean Threat Groups **(Unit 42)**