

Espionage

Sunburst used in SolarWinds attack (2020)

- Considered one of the most sophisticated supply-chain intrusions
- Impacted US government agencies and Fortune 500 companies
- Believed to be originated from China

Volt Typhoon (2023)

- Targeted US critical infrastructure: telecom, energy, water, transportation
- Believed to be originated from China

Sabotage

Shamoon (2012)

- Targeted oil and gas infrastructure in Qatar and Saudi Arabia
- Destroyed 30,000 machines

CrashOverride (2015)

- Targeted the Ukrainian Power Grid
- First malware to turn off electricity at scale