Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:23:40 UTC

(Wikipedia) The Central Intelligence Agency is a civilian foreign intelligence service of the federal government of the United States, tasked with gathering, processing, and analyzing national security information from around the world, primarily through the use of human intelligence (HUMINT). As one of the principal members of the United States Intelligence Community (IC), the CIA reports to the Director of National Intelligence and is primarily focused on providing intelligence for the President and Cabinet of the United States.

(Yahoo) In September 2018, Bolton announced that Trump had signed a presidential directive easing Obama-era rules governing military cyber operations. Although the administration disclosed the existence of that directive — known as National Security Presidential Memorandum 13 — the underlying rules of engagement for military cyber operations remain secret. The administration also kept secret the CIA finding, which gave the agency its new authorities.

Former officials declined to speak in detail about cyber operations the CIA has carried out as a result of the finding, but they said the agency has already conducted covert hack-and-dump actions aimed at both Iran and Russia.

This more permissive environment may also intensify concerns about the CIA's ability to secure its hacking arsenal. In 2017, WikiLeaks published a large cache of CIA hacking tools known as "Vault 7" (see [Vault 7/8].) The leak, which a partially declassified CIA assessment called "the largest data loss in CIA history," was made possible by "woefully lax" security practices at the CIA's top hacker unit, the assessment said.

The CIA was also one of the parties involved in Operation Olympic Games where Stuxnet was deployed in Iran.

While not strictly related to APT activity and not just involving the CIA, the following publication in 3 parts sheds more light:
1. <https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/>
2. <https://foreignpolicy.com/2020/12/22/china-us-data-intelligence-cybersecurity-xi-jinping/>
3. <https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/>

The CIA has 2 subgroups:
1. Subgroup: Longhorn, The Lamberts.
2. Subgroup: [Unnamed group USA].
