

Operation Shady RAT

By Contributors to Wikimedia projects

Published: 2011-08-03 · Archived: 2026-04-05 20:39:25 UTC

From Wikipedia, the free encyclopedia

Operation Shady RAT is an ongoing series of [cyber attacks](#) starting in mid-2006^[1] reported by [Dmitri Alperovitch](#), Vice President of Threat Research at Internet security company [McAfee](#) in August 2011, who also led and named the [Night Dragon Operation](#) and [Operation Aurora cyberespionage](#) intrusion investigations.^[2] The attacks have hit at least 71 organizations, including [defense contractors](#), businesses worldwide, the [United Nations](#), and the [International Olympic Committee](#).^{[3][4]} Governments attacked include Canada, India, South Korea, Taiwan, United States, and Vietnam. International bodies attacked include the United Nations, the Association of Southeast Asian Nations (ASEAN), the International Olympic Committee, and the World Anti-Doping Agency.^[5]

The operation, named by Alperovitch as a derivation of the common computer security industry acronym for [remote access tool](#), is characterized by McAfee as "a five-year targeted operation by one specific actress". The report suggests that the targeting of various athletic oversight organizations around the time of the [2008 Summer Olympics](#) "potentially pointed a finger at a state actor behind the intrusions".^[2] That state actor is widely assumed to be the [People's Republic of China](#).^[6]

The hackers sent phishing emails, which were tainted with malicious software, to specific people at the targeted organizations. If the unsuspecting receiver of the mail clicked on the attached malicious software, it would infect their computer which in turn would give the hacker access to their computer.^[5]

- [Cyberwarfare and China](#)
- [Advanced persistent threat](#)
- [DigiNotar](#)
- [Duqu](#)
- [PLA Unit 61398](#)
- [Tailored Access Operations](#)

1. [^] Jim Finkle (2011-08-03). ["State actor seen in "enormous" range of cyber attacks"](#). *Reuters*. Retrieved 2011-08-03.
2. [^] [Jump up to: ^a ^b](#) Dmitri Alperovitch (2011-08-02). ["Revealed: Operation Shady RAT"](#) (PDF). *McAfee*. Archived from [the original](#) (PDF) on 2011-08-04. Retrieved 2011-08-03.
3. [^] ["Governments, IOC and UN hit by massive cyber attack"](#). *BBC News*. 2011-08-03. Retrieved 3 August 2011.
4. [^] Nakashima, Ellen, ["Report on 'Operation Shady RAT' identifies widespread cyber-spying"](#), *Washington Post*, 3 August 2011.

5. ^ [Jump up to: ^a ^b](#) ["Q+A: Massive cyber attack dubbed "Operation Shady RAT"". Reuters. 2011-08-03. Retrieved 2023-11-02.](#)
6. [^] Gross, Michael Joseph, ["Enter the Cyber-dragon"](#), *Vanity Fair*, September 2011.

Source: https://en.wikipedia.org/wiki/Operation_Shady_RAT