PLA Unit 61398

AFFILIATIONS

Also known as APT 1, Comment Crew, Comment Panda, TG-8223, Group 3, GIF89a, and Byzantine Candor

U.S. cybersecurity firm Mandiant, later purchased by FireEye, released a report (https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html) in February 2013 that exposed one of China's cyber espionage units, Unit 61398. The group, which FireEye called APT 1, is a unit within China's People's Liberation Army (PLA) that has been linked to a wide range of cyber operations targeting U.S. private sector entities for espionage purposes. The comprehensive report detailed evidence connecting APT 1 and the PLA, offered insight into APT 1's operational malware and methodologies, and provided timelines of the espionage it conducted. FireEye termed Unit 61398 "APT 1" to indicate that the threat actor was an Advanced Persistent Threat (https://www.fireeye.com/blog/executive-perspective/2014/04/apt1-the-state-of-the-hack-one-year-later.html), a type of operation in which the goal of the network intrusion is not only to gain access to a server or system, but also to retain ongoing access and engage in protracted cyber operations. The APT 1 report exposed the infrastructure of a cyber threat actor and gave both government and nongovernment organizations insight into the escalating nature of state-sponsored cyber operations.

SUSPECTED VICTIMS

United States

Taiwan

Israel

Norway

United Arab Emirates

United Kingdom

Singapore

India

Belgium

South Africa

Switzerland

Canada

France

Luxembourg

Japan

SUSPECTED STATE SPONSOR

China

TYPE OF INCIDENT

Espionage

TARGET CATEGORY

Private sector

Government

READ MORE

APT 1: Exposing One of China's Cyber Espionage Units (https://web.archive.org/web/20130219155150/http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)

Operation Shady RAT (http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf)

Chinese Army Unit Is Seen as Tied to Hacking Against U.S. (http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html)