PLA Unit 61398

By Contributors to Wikimedia projects

Published: 2013-02-19 · Archived: 2026-04-05 14:08:37 UTC

People's Liberation Army Unit 61398	
61398部队	
 Emblem of the People's Liberation Army	
Active	2002–present
Country	China
Allegiance	Chinese Communist Party
Branch	People's Liberation Army Cyberspace Force
Type	Cyber force, Cyber-espionage Unit
Role	Cyber warfare Electronic warfare
Part of	People's Liberation Army
Garrison/HQ	Tonggang Road, Pudong, Shanghai
Nicknames	• APT 1 • Comment Crew • Comment Panda • GIF89a

	• Byzantine Candor • Group 3 • Threat Group 8223
Engagements	• Operation GhostNet • Operation Aurat • Operation Shady RAT

PLA Unit 61398 (also known as **APT1**, **Comment Crew**, **Comment Panda**, **GIF89a**, or **Byzantine Candor**; Chinese: 61398部队, Pinyin: 61398 *bùduì*) is the military unit cover designator (MUCD)[1] of a People's Liberation Army advanced persistent threat unit that has been alleged to be a source of Chinese computer hacking attacks.[2][3][4] The unit is stationed in Pudong, Shanghai,[5] and has been cited by US intelligence agencies since 2002.

From left, Chinese military officers Gu Chunhui, Huang Zhenyu, Sun Kailiang, Wang Dong, and Wen Xinyu indicted on cyber espionage charges.

A report by the computer security firm Mandiant stated that PLA Unit 61398 is believed to operate under the 2nd Bureau of the People's Liberation Army General Staff Department (GSD) Third Department (总参三部二局)[1] and that there is evidence that it contains, or is itself, an entity Mandiant calls APT1, part of the advanced persistent threat that has attacked a broad range of corporations and government entities around the world since at least 2006. APT1 is described as comprising four large networks in Shanghai, two of which serve the Pudong New Area. It is one of more than 20 APT groups with origins in China.[1][6] The Third and Fourth Department, responsible for electronic warfare, are believed to comprise the PLA units mainly responsible for infiltrating and manipulating computer networks.[7]

On 19 May 2014, the US Department of Justice announced that a federal grand jury had returned an indictment of five 61398 officers on charges of theft of confidential business information and intellectual property from U.S. commercial firms and of planting malware on their computers.[8][9] The five are Huang Zhenyu (黄振宇), Wen Xinyu (文新宇), Sun Kailiang (孙凯亮), Gu Chunhui (顾春晖), and Wang Dong (王东). Forensic evidence traces the base of operations to a 12-story building off Datong Road in a public, mixed-use area of Pudong in Shanghai.[2] The group is also known by various other names including "Advanced Persistent Threat 1" ("APT1"), "the Comment group" and "Byzantine Candor", a codename given by US intelligence agencies since 2002.[10][11][12][13]

The group often compromises internal software "comment" features on legitimate web pages to infiltrate target computers that access the sites, leading it to be known as "the Comment Crew" or "Comment Group".[15] The

collective has stolen trade secrets and other confidential information from numerous foreign businesses and organizations over the course of seven years such as Lockheed Martin, Telvent, and other companies in the shipping, aeronautics, arms, energy, manufacturing, engineering, electronics, financial, and software sectors.[11]

Dell SecureWorks says it believed the group includes the same group of attackers behind Operation Shady RAT, an extensive computer espionage campaign uncovered in 2011 in which more than 70 organizations over a five-year period, including the United Nations, government agencies in the United States, Canada, South Korea, Taiwan and Vietnam, were targeted.[2]

The attacks documented in the summer of 2011 represent a fragment of the Comment group's attacks, which go back at least to 2002, according to incident reports and investigators. In 2012, FireEye, Inc. stated that they had tracked hundreds of targets in the last three years and estimated the group had attacked more than 1,000 organizations.[12]

Most activity between malware embedded in a compromised system and the malware's controllers takes place during business hours in Beijing's time zone, suggesting that the group is professionally hired, rather than private hackers inspired by patriotic passions.[7]

A 2020 report in Daily News and Analysis stated that the unit was eyeing information related to defense and research in India.[16]

Public position of the Chinese government

[edit]

Until 2013, the government of China has consistently denied that it is involved in hacking.[17] In response to the Mandiant Corporation report about Unit 61398, Hong Lei, a spokesperson for the Chinese foreign ministry, said such allegations were "unprofessional".[17][4]

- Titan Rain
- Chinese espionage in the United States
- National Security Agency of the United States
- PLA Unit 61486
- Signals intelligence
- Tailored Access Operations of the United States
- Mandiant
- FireEye

1. ^ Jump up to: *a* *b* *c* *"APT1: Exposing One of China's Cyber Espionage Units"* (PDF). Mandiant. *Archived* (PDF) from the original on 19 February 2013. Retrieved 19 February 2013.
2. ^ Jump up to: *a* *b* *c* Sanger, David E.; Barboza, David; Perlroth, Nicole (19 February 2013). *"Chinese Army Unit Is Seen as Tied to Hacking Against U.S."* *The New York Times*. *ISSN* *0362-4331*. *Archived* from the original on 19 February 2013. Retrieved 28 May 2023.

3. ^ *"Chinese military unit behind 'prolific and sustained hacking'"*. *The Guardian*. *19 February 2013. Archived from the original on 20 December 2013. Retrieved 19 February 2013.*
4. ^ Jump up to: *a b* *"Hello, Unit 61398"*. *The Economist*. *19 February 2013. ISSN 0013-0613. Archived from the original on 28 May 2023. Retrieved 28 May 2023.*
5. ^ *"中国人民解放军61398部队招收定向研究生的通知" [A notification of PLA Unit 64398 to recruit postgraduate students as PLA-funded scholarship student.]. Zhejiang University. 13 May 2004. Archived from the original on 2 December 2016. Retrieved 5 January 2019.*
6. ^ *Joe Weisenthal and Geoffrey Ingersoll (18 February 2013). "REPORT: An Overwhelming Number Of The Cyber-Attacks On America Are Coming From This Particular Army Building In China". Business Insider. Archived from the original on 20 February 2013. Retrieved 19 February 2013.*
7. ^ Jump up to: *a b* *Bodeen, Christopher (25 February 2013). "Sign That Chinese Hackers Have Become Professional: They Take Weekends Off". The Huffington Post. Archived from the original on 26 February 2013. Retrieved 27 February 2013.*
8. ^ Finkle, J., Menn, J., Viswanatha, J. *U.S. accuses China of cyber spying on American companies.* Archived 12 April 2017 at the Wayback Machine Reuters, 20 Nov 2014.
9. ^ Clayton, M. *US indicts five in China's secret 'Unit 61398' for cyber-spying.* Archived 20 May 2014 at the Wayback Machine Christian Science Monitor, 19 May 2014
10. ^ *David Perera (6 December 2010). "Chinese attacks 'Byzantine Candor' penetrated federal agencies, says leaked cable". fiercegovernmentit.com. Fierce Government IT. Archived from the original on 19 April 2016.*
11. ^ Jump up to: *a b* *Clayton, Mark (14 September 2012). "Stealing US business secrets: Experts ID two huge cyber 'gangs' in China". CSMonitor. Archived from the original on 15 November 2019. Retrieved 24 February 2013.*
12. ^ Jump up to: *a b* *Riley, Michael; Dune Lawrence (26 July 2012). "Hackers Linked to China's Army Seen From EU to D.C." Bloomberg.com. Bloomberg. Archived from the original on 11 January 2015. Retrieved 24 February 2013.*
13. ^ *Michael Riley; Dune Lawrence (2 August 2012). "China's Comment Group Hacks Europe—and the World". Bloomberg Businessweek. Archived from the original on 19 February 2013. Retrieved 12 February 2013.*
14. ^ *Dave Lee (12 February 2013). "The Comment Group: The hackers hunting for clues about you". BBC News. Archived from the original on 12 February 2013. Retrieved 12 February 2013.*
15. ^ *Shukla, Manish (3 August 2020). "Chinese Army's secret '61398' unit spying on India's defense and research, warns intelligence". DNA India. Archived from the original on 20 November 2022. Retrieved 6 January 2024.*
16. ^ Jump up to: *a b* *Xu, Weiwei (20 February 2013). "China denies hacking claims". Morning Whistle. Retrieved 8 April 2013.* `{{cite web}}` : CS1 maint: deprecated archival service (link)

31°20′57.43″N 121°34′24.74″E / 31.3492861°N 121.5735389°E
