PLA Unit 61398

en.wikipedia.org/wiki/PLA_Unit_61398

Contributors to Wikimedia projects

This article **may be expanded with text translated from the corresponding article in Chinese**. *(February 2013)* Click [show] for important translation instructions.

- View a machine-translated version of the Chinese article.
- Machine translation like DeepL or Google Translate is a useful starting point for translations, but translators must revise errors as necessary and confirm that the translation is accurate, rather than simply copy-pasting machine-translated text into the English Wikipedia.
- Consider **adding a topic** to this template: there are already 772 articles in the main category, and specifying `|topic=` will aid in categorization.
- Do not translate text that appears unreliable or low-quality. If possible, verify the text with references provided in the foreign-language article.
- You **must** provide copyright attribution in the edit summary accompanying your translation by providing an interlanguage link to the source of your translation. A model attribution edit summary is `Content in this edit is translated from the existing Chinese Wikipedia article at [[:zh:解放軍61398部隊]]; see its history for attribution.`
- You should also add the template `{{Translated|zh|解放軍61398部隊}}` to the talk page.
- For more guidance, see Wikipedia:Translation.

People's Liberation Army Unit 61398

61398部队

Country	People's Republic of China
Branch	People's Liberation Army Strategic Support Force
Type	Cyber force
Role	Cyber warfare Electronic warfare
Garrison/HQ	Tonggang Road, Pudong, Shanghai

Nickname(s)	• 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 **APT 1**, **Comment Crew**, **Comment Panda**, **GIF89a**, and **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] The unit is stationed in Pudong, Shanghai.[4]

History

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

See also: Chinese information operations and information warfare

2014 indictment

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.[5][6] 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.[7][8][9][10]

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][11] The Third and Fourth Department, responsible for electronic warfare, are believed to comprise the PLA units mainly responsible for infiltrating and manipulating computer networks.[12]

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".[13][14] 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.[8]

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. FireEye, Inc. alone has tracked hundreds of targets in the last three years and estimates the group has attacked more than 1,000 organizations.[9]

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.[12]

Public position of the Chinese government

Until 2013, the Government of China has consistently denied that it is involved in hacking.[15] In response to the Mandiant Corporation report about Unit 61398, Hong Lei, a spokesperson for the Chinese foreign ministry, said such allegations were "unprofessional".[15][16]

In 2013, China changed its position and openly admitted to having secretive cyber warfare units in both the military and the civilian part of the government – however, the details of their activities were left to speculation.[17] As a show of force towards the rest of the global community the Chinese government now openly lists their abilities when it comes to digital spying and network attack capabilities.[18]

Cultural references

In the 2022 cyber thriller Rise of the Water Margin, which is a 21st century adaptation of the classic Water Margin Unit 61398 is commanded by Lin Chong. His team infiltrates semiconductor EDA tools in order to embed a back door into semiconductors.

See also

- 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

References

1. ^ 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. ^ a b c *David E. Sanger, David Barboza and Nicole Perlroth (18 February 2013). "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." New York Times. Archived from the original on 22 February 2013. Retrieved 19 February 2013.*
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. ^ *"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.*
5. ^ 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.
6. ^ 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
7. ^ *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.*
8. ^ 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.*
9. ^ 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.*

10. ^ 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.
11. ^ 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.
12. ^ 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.
13. ^ Martin, Adam (19 February 2013). "Meet 'Comment Crew,' China's Military-Linked Hackers". NYMag.com. New York Media. Archived from the original on 22 February 2013. Retrieved 24 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. ^ a b Xu, Weiwei (20 February 2013). "China denies hacking claims". Morning Whistle. Archived from the original on 29 June 2013. Retrieved 8 April 2013.
16. ^ "Hello, Unit 61398". The Economist. 19 February 2013. Archived from the original on 5 March 2013. Retrieved 5 March 2013.
17. ^ "China Finally Admits focusing on Cyber Warfare" (PDF). 19 March 2015. Archived (PDF) from the original on 29 August 2017. Retrieved 13 September 2017.
18. ^ BBC (7 May 2013). "US accuses China government and military of cyber-spying". BBC News. Archived from the original on 15 January 2019. Retrieved 15 January 2019.

Hacking in the 2000s

Timeline

Incidents	2004	• Titan Rain (2003–2006) • Operation Firewall
	2007	• Cyberattacks on Estonia • Operation: Bot Roast
	2008	• Project Chanology • Cyberattacks on Georgia • Sarah Palin email hack • US Military Cyberattack
	2009	• Operation Troy • WebcamGate (2008–2010)
Groups		
Individuals		
Vulnerabilities discovered		
Malware	2000	• ILOVEYOU • Pikachu
	2001	• Anna Kournikova • Code Red • Nimda • Klez
	2002	Simile
	2003	• SQL Slammer • Welchia • Sobig • Gruel • Blaster

2004	- Bagle - NetSky - Sasser - Mydoom
2005	- PGPCoder - Samy
2006	- Rostock - ZLOB - Stration
2007	- Storm - ZeuS
2008	- Asprox - Patched - Agent.btz - Mariposa
2009	- Conficker - Koobface - Waledac

Hacking in the 2010s

Timeline

Major incidents

2010	- Operation Aurora - Australian cyberattacks - Operation ShadowNet - Operation Payback

2011	DigiNotar DNSChanger HBGary Federal Operation AntiSec Operation Tunisia PlayStation RSA SecurID compromise
2012	LinkedIn hack Stratfor email leak Operation High Roller
2013	South Korea cyberattack Snapchat hack Cyberterrorism Attack of June 25 2013 Yahoo! data breach Singapore cyberattacks
2014	Anthem medical data breach Operation Tovar 2014 celebrity nude photo leak 2014 JPMorgan Chase data breach Sony Pictures hack Russian hacker password theft 2014 Yahoo! data breach
2015	Office of Personnel Management data breach Hacking Team Ashley Madison data breach VTech data breach Ukrainian Power Grid Cyberattack SWIFT banking hack
2016	Bangladesh Bank robbery Hollywood Presbyterian Medical Center ransomware incident Commission on Elections data breach Democratic National Committee cyber attacks Vietnam Airport Hacks DCCC cyber attacks Indian Bank data breaches Surkov leaks Dyn cyberattack Russian interference in the 2016 U.S. elections 2016 Bitfinex hack

	2017	• 2017 Macron e-mail leaks • WannaCry ransomware attack • Westminster data breach • Petya cyberattack 2017 cyberattacks on Ukraine • Equifax data breach • Deloitte breach • Disqus breach
	2018	• Trustico • Atlanta cyberattack • SingHealth data breach
	2019	• Sri Lanka cyberattack • Baltimore ransomware attack • Bulgarian revenue agency hack • Jeff Bezos phone hacking
Hacktivism		
Advanced persistent threats		
Individuals		
Major vulnerabilities publicly disclosed		
Malware		
	2010	• Bad Rabbit • SpyEye • Stuxnet
	2011	• Alureon • Duqu • Kelihos • Metulji botnet • Stars

2012	Carna Dexter FBI Flame Mahdi Red October Shamoon
2013	CryptoLocker DarkSeoul
2014	Brambul Carbanak Careto DarkHotel Duqu 2.0 FinFisher Gameover ZeuS Regin
2015	Dridex Hidden Tear Rombertik TeslaCrypt
2016	Hitler Jigsaw KeRanger MEMZ Mirai Pegasus Petya (NotPetya) X-Agent
2017	BrickerBot Kirk LogicLocker *Rensenware* ransomware Triton WannaCry XafeCopy

- Grum
- Joanap
- NetTraveler
- R2D2
- Tinba
- Titanium
- Vault 7
- ZeroAccess botnet

2019

National security and law enforcement in China

National organizations

Mainland organizations

Hong Kong organizations

Macau organizations

Operations

Other topics

Coordinates: 31°20′57.43″N 121°34′24.74″E