PLA Unit 61486

By Contributors to Wikimedia projects

Published: 2014-06-10 · Archived: 2026-04-05 22:05:13 UTC

From Wikipedia, the free encyclopedia

Unit 61486	
Country	China
Allegiance	Chinese Communist Party[1]
Branch	People's Liberation Army Cyberspace Force
Type	Cyber force
Role	Cyber warfare Electronic warfare
Part of	People's Liberation Army
Nickname	Putter Panda

PLA Unit 61486 (also known as **Putter Panda** or **APT2**) is a People's Liberation Army unit dedicated to executing cyberattacks on American, Japanese, and European corporations focused on satellite and communications technology. It is a unit that takes part in China's campaign to steal trade and military secrets from foreign targets.[2][3][4][5]

In 2014, they were exposed to the public by a report made by CrowdStrike, a digital security firm. One member of Unit 61486 has been identified as Chen Ping, with the online alias of "cpyy". Unit 61486 has also been nicknamed "Putter Panda" by the security firm Crowdstrike, in reference to its Chinese origins ("panda") and its penchant for targeting golf players ("putter").[2]

Its exposure came after another PLA unit, PLA Unit 61398, was exposed for similar activity, the previous year, as well as the indictment of five members of Unit 61398 by the United States the previous month.[2] Meanwhile, Edward Snowden's release of information on America's surveillance program would also become a focal point in China's response to the accusations of spying, using it as evidence the United States was hypocritical in their accusations of espionage.[6]

Unit 61486 is a bureau within the Operations arm of the Third Department of the General Staff Department. Its name, Unit 61486, is a Military Unit Cover Designator (MUCD), these are used to hide the unit's true identity.[7] The earliest signs of the unit's existence comes from 2007.[8] Unit 61486 is the 12th Bureau within the Third

Department, the majority of their cyber attacks have been focused on targeting American, European, and Japanese industries that worked in aerospace and satellite. They are believed to be focused on space technology.[7][8]

They primarily have done their work through a technique known as spear-phishing, also known as Remote Access Tools (RAT), targeting members of industries noted above, specifically members that had played golf as major targets in their operations.[2] They would use emails that had PDF and word documents that detailed information related to conferences, from there the Remote Access Tool would be installed allowing for the victims computer to be accessed.[5] An example of this operation can be seen when an email brochure that appeared to be for a yoga studio in Toulouse would steal the personal information of the person who opened the email.[2] From Crowdstrike's report, they claim that the Unit 61486 used the Adobe Reader and Microsoft office as the vessels for the malware.[6] According to Crowdstrike, the attack on the Canadian National Research Council in 2014 could also be attributed to Unit 61486. Crowdstrike's Chief Technology Officer Dmitri Alperovitch would say that the attack was similar to ones that had been conducted by Unit 61486 in the past, claiming "It certainly looks like one of the actors we track out of China that we've seen going after aircraft manufacturers in the past,".[9] However, Canada has only stated the attack was done by state actors working for China, saying "a highly sophisticated Chinese state-sponsored actor" had been responsible for the attack. Their statement did not directly attribute it to Unit 61486.[7][9]

In response to these allegations, Ministry of Foreign Affairs of the People's Republic of China would demand that Canada stop making these claims. Foreign ministry spokesman Qin Gang said that they did not have any evidence to back this claim and this accusation was unjustified provocation.[9]

Exposing of Operations

[edit]

Zhabei District from Pearl Tower, where Unit 61486's headquarters is believed to be located

On the 9th of June 2014, the security firm Crowdstrike released a report detailing the actions of Unit 61486, as well as a potential member of the unit.[8] Crowdstrike states the reason for releasing this report publicly was because of China's statement following the United States indictment of 5 members in Unit 61398. China responded to the indictment claiming these were lies, and that the information used was fabricated.[8][6] The CEO of Crowdstrike, George Kurtz states they publicly released the report to provide irrefutable evidence of China's involvement with cyber espionage, as a means to counter the claims made by the Chinese government.:[5]

> "This report is part of our extensive intelligence library and was made available to our intelligence subscribers in April 2014, prior to the US Government's criminal indictment and China's subsequent refusal to engage in a constructive dialog ... We believe the U.S. Government indictments and global acknowledgment and awareness are important steps in the right direction. In support of these efforts, we are making this report available to the public to continue the dialog around this ever-present threat."[8]

Another aim of releasing the report was to show the international community that the indictment of 5 individuals for cyber espionage was limit of China's cyber espionage program, or that this program was limited to targeting only the United States. Rather it was just "the tip of the iceberg" as George Kurtz wrote, with campaigns taking place across the world.[8]

The investigation revealed a potential member of the unit under the alias "cpyy". Several emails that used this alias were registered to a person name Chen Ping. On a personal blog on 163.com, it lists this persons employment as either military or police, it also lists his birth date as 25 May 1979. The same page also had posts in an IT category, whilst related a separate blog linked to Chen Ping indicated he had either studied or worked on networking or programming from 2002 to 2003. This report also pointed to several images on their personal sina.com blog that said they had attended Shanghai Jiao Tong University, a university that allegedly is targeted for recruitment into the PLA. In addition, several other posts suggested he was a member of the PLA, from photos with PLA uniforms in the background.[10][8] In a personal blog Chen Ping listed his work as military, whilst in a different blog, a post said "Soldier's duty is to defend the country, as long as our country is safe, our military is excellent.", suggesting that Chen held nationalistic ideals that would encourage one to join the armed forces. This blog also states that Chen Ping lived in Shanghai from 2005 to 2007. However, this page was last updated in 2007 before being taken down following the release of Crowdstrike's report.[8]

Based on previous IP addresses and photos from Chen Ping's multiple personal blogs, Crowdstrike states that the headquarters for the unit is within the Zhabei District of Shanghai. Furthermore, several of the website domains registered by Chen Ping led to an address that was close to a building he took a photo of, and posted under the caption of "office". Additionally, these personal photos showed large satellite dish installations. From Crowdstrike's investigations they believed that Unit 61486 was involved in space surveillance and also the targeting of western companies that manufactured or researched satellites. Thus the satellite dishes were related to this activity. A webpage published by a Chinese government entity that details theatrical performances involving members of the PLA listed an address that also corresponds to an area that has the buildings in Chen Ping's photos. With the address from this site as well as the personal photos from Chen Pings blogs, Crowdstrike states that they believe that this building is the headquarters for Unit 61486.[10][8]

This report also suggested that Unit 61486 works alongside Unit 61398, another unit within the Third Department. Several domains registered to alleged members of 61486 have the same IP address as ones from Unit 61398. In addition to the allegations of cooperation with Unit 61398, another unit, Vixen Panda, is mentioned to have a connection to unit 61486, as an IP address that had been used by Vixen Panda for one of their sites had also been associated with a domain that Unit 61486 had used. Furthermore, "cpyy" (Chen Ping) was also found to interact with an individual listed as "linxder", on cpyy.org, cpyy's site. The individual Linxder is the handle of someone part of Comment Panda, another hacking group believed to be in Shanghai.[8]

Following the exposing of Chen Ping or "cpyy", his information was all taken down the day after the report was released. Additionally, according to Crowdstrike they believe that Chen Ping has been moved from Shanghai to Kunming in Yunnan province. According to the Project 2049 Institute, the Unit 61486 has a facility in the region. [*citation needed*]

This report had been available to subscribers of Crowdstrike since April 2014 However, only following the public release of the report would there be responses made by the United States as well as the Chinese Foreign Ministry. [10]

Official Response by the Chinese Foreign Ministry

[edit]

In the previous year, the security firm Mandiant had exposed Unit 61398, for doing similar activity to Unit 61486. The month before the report on Unit 61486 was released, the United States had indicted 5 people they believed to be members of Unit 61398, of cyber espionage, marking the first time this charge was levelled at state actors.[5] The exposing of Unit 61486 raised tensions between the two nations higher. This led to the Foreign Ministry threatening to start a trade war with the United States, as well as more inspections and regulations of US Technologies coming into the country.[2] Additionally, China would pull out of several meetings with the United States over the issue of hacking. Additionally, a spokeswoman for China's foreign ministry upon hearing the allegations over Unit 61486 listed by Crowdstrike's report scorned it as giving her "déjà vu", in reference to the report made by Mandiant the year before.[6]

Edward Snowden had exposed the United States spying programs conducted by the CIA and NSA the year before Unit 61486 was revealed by the Crowdstrike report. This was brought up by Foreign Ministry spokeswoman Hua Chunying, as an example of the United States being hypocritical in their accusations of China stealing information from Western corporations. Spokeswoman Hua Chunying would state that the United States had no right to accuse others of hacking, as they had been caught doing so. She stated that the United States is a "Hacker empire".[2][6]

> In a Press conference Foreign Ministry spokeswoman Hua Chunying states "The United States cannot pretend that it is the victim. They are a hacker empire. I think everyone in the world knows this."[6]

In addition, earlier in the year it was revealed by *The New York Times* and *Der Spiegel* that the NSA had also hacked Huawei's servers. This was done to see if there was any relationship between the PLA and Huawei, however it quickly expanded to developing exploits that would allow the NSA to access their networks to conduct surveillance and "offensive operations". This operation known as "Shotgiant" was conducted despite a House Intelligence Committee report in 2012 stated that there was no connection between the PLA and Huawei, along with another entity known as ZTF. This also was brought up by the Foreign Ministry as another case of American hypocrisy in spying allegations.[11] The Foreign Ministry Spokesperson further iterated that the report could not be correct, saying it was ridiculous that someone that would do this sort of work would be open about being a hacker.

> In a news brief, Foreign Ministry spokeswoman Hua Chunying states:"I think this is both curious and puzzling. Have you ever seen a thief in the street who advertises on his chest that he is a thief? Honestly

> speaking, I think what the U.S. has done here cannot be accepted as correct."[6]

In addition to these allegations, the week before the report was released, the Chinese government criticised the United States Department of Defense for releasing a report that said they believed China's actual military spending was an estimated $145 billion US dollars. The report additionally warned that China was speeding up its military modernisation program. However, even though tensions and relations between the two nations were already poor, and increasing from these events and allegations, China would still accept an invitation to participate in RIMPAC which was to occur within the month. This would mark the first time China would participate in an American led naval drill, though they had previously participated in 1998 as observers. They would send 4 ships in total, a destroyer, frigate, a supply ship and a hospital ship.[6][12]

- PLA Unit 61398
- Chinese information operations and information warfare

1. ^ *"The PLA Oath" (PDF). Defense Technical Information Center. February 2009. Archived (PDF) from the original on September 24, 2015. Retrieved October 30, 2015. "I am a member of the People's Liberation Army. I promise that I will follow the leadership of the Communist Party of China..."*
2. ^ Jump up to: **a b c d e f g** *Perlroth, Nicole (9 June 2014). "2nd China Army Unit Implicated in Online Spying". The New York Times. Archived from the original on 10 June 2014. Retrieved 9 June 2014.*
3. ^ *"Second China unit accused of cyber crime". Financial Times. 10 June 2014. Archived from the original on 30 April 2024. Retrieved 10 June 2014.*
4. ^ *"Cyber Spies Targeting U.S. Defense, Tech Firms Linked to China's PLA: Report". SecurityWeek.com. Archived from the original on 28 December 2017. Retrieved 18 December 2017.*
5. ^ Jump up to: **a b c d** *"Cyber conflict escalates: Second Chinese PLA hacking group accused -". Defense Systems. Archived from the original on 28 December 2017. Retrieved 18 December 2017.*
6. ^ Jump up to: **a b c d e f g h** *Menn, Joseph (10 June 2014). "Private U.S. report accuses another Chinese military unit of hacking". Reuters. Archived from the original on 17 October 2020. Retrieved 15 October 2020.*
7. ^ Jump up to: **a b c** *Cheng, Dean (14 November 2016). Cyber Dragon:Inside China's Information Warfare and Cyber Operations. ABC-CLIO, LLC, 2017. ISBN 978-1440835643.*
8. ^ Jump up to: **a b c d e f g h i j** *"Crowdstrike Intelligence Report: Putter Panda" (PDF). Crowd Strike. Archived (PDF) from the original on 11 November 2020. Retrieved 2 November 2020.*
9. ^ Jump up to: **a b c** *Sharp, Alastaire; Ljunggren, David (1 August 2014). "Hacking attack in Canada bears signs of Chinese army unit: expert". Reuters. Archived from the original on 16 May 2021. Retrieved 2 November 2020.*
10. ^ Jump up to: **a b c** *Frizell, Sam. "How to Hunt a Chinese Hacker". Time Magazine. Archived from the original on 2021-01-22. Retrieved 2020-11-02.*
11. ^ *Perloth, Nicole; Sanger, David (22 March 2014). "N.S.A. Breached Chinese Servers Seen as Security Threat". The New York Times. The New York Times. Archived from the original on 18 February 2017. Retrieved 2 November 2020.*
12. ^ *"China confirms attendance at U.S.-hosted naval exercises in June". Reuters. 9 June 2014. Archived from the original on 8 March 2020. Retrieved 2 November 2020.*

Source: https://en.wikipedia.org/wiki/PLA_Unit_61486