China’s PLA Unit 61419 Purchasing Foreign Antivirus Products, Likely for Exploitation

recordedfuture.com/china-pla-unit-purchasing-antivirus-exploitation/

Insikt Group

Recorded Future’s Insikt Group has discovered six procurement documents from official People’s Liberation Army (PLA) military websites and other sources that show the Strategic Support Force (SSF) branch of the PLA, specifically Unit 61419, has sought to purchase antivirus software from several major American, European, and Russian security companies. The PLA’s Unit 61419 sought to purchase English-language versions of the security software listed below (Table 1). The focus on English versions of these products is notable because Chinese-language versions would be the more logical choice if the software was intended for legitimate use or to test the potential exposure of private and commercial end-users in China to vulnerabilities in foreign antivirus software.

Insikt Group assesses that the purchase of foreign antivirus software by the PLA poses a high risk to the global antivirus software supply chain. Based on patterns of past campaigns and tactics, two scenarios are most likely for the PLA’s exploitation of foreign antivirus software:

Scenario 1: PLA cyber units and affiliated hacking groups will use foreign antivirus programs as a testing environment for natively developed malware. They will run the malware through foreign antivirus products to test its ability to evade detection, thereby making it more likely to successfully infect its targeted victims.

Scenario 2: PLA cyber units and affiliated hacking groups will reverse engineer the foreign antivirus software code to find previously undisclosed vulnerabilities. They will then use the newly discovered vulnerabilities in a zero-day attack for initial intrusion.

Date of Procurement Order	Product Name	Subscription Length	Number of Users	Country of Supplier

January 2019	Kaspersky Security Cloud Family	1 year	20 user terminals	Russia
January 2019	Kaspersky Security Cloud Personal	1 year	10 user terminals	Russia
January 2019	Kaspersky Endpoint Security for Business Select	1 year	10 user terminals	Russia
January 2019	Kaspersky Endpoint Security Cloud Plus	1 year	10 user terminals	Russia
January 2019	Avira Prime	1 year	10 user terminals	Germany
April-May 2019	Kaspersky Endpoint Security for Business ADVANCED	2 years	30 user terminals	Russia
April-May 2019	McAfee Total Protection	2 years	30 user terminals	US
April-May 2019	Dr. Web Enterprise Security Suite	2 years	30 user terminals	Russia
April-May 2019	Nod32 ESET Multi-Device Security	2 years	10 user terminals	Slovakia
April-May 2019	Norton Security Premium	2 years	10 user terminals	US
April-May 2019	Symantec Endpoint Protection Subscription	2 years	10 user terminals	US
November 2019	Trend Micro Worry-Free Services Advanced	2 years	10 user terminals	US-Japan
November 2019	Sophos Intercept X	2 years	10 user terminals	UK
November 2019	BitDefender Total Security	2 years	10 user terminals	Romania

Table 1: *Antivirus security software included in the procurement documents discovered by Insikt Group*

Insikt Group also found a contract award announcement published by the SSF related to the acquisition of Cisco routers, among other pieces of communications technology. This document uses the same contact address associated with Unit 61419 as many of the antivirus procurement documents.

Figure 1 below is a sample screenshot of a product list obtained from a Chinese military procurement website:

Figures 1: *Unit 61419 procurement document product list*

Patterns of Past Campaigns

Several factors inform our assessment that the purchase of English-language foreign antivirus software is motivated by SSF's role in computer network exploitation by the Chinese military:

China has demonstrated a pattern of software supply chain exploitation in multiple cyber intrusion campaigns, including against some of the foreign antivirus software purchased in 2019.

1. In 2017, over 2.27 million users of **Avast CCleaner** were compromised by a malicious update planted by a Chinese state-sponsored threat actor, resulting in over 1.6 million computers being infected with the first-stage Floxif trojan. A small subset of those victims was infected with a second-stage trojan, likely for espionage.
2. In the summer of 2019, a Chinese state-sponsored APT called Tick Group exploited two zero-days impacting **Trend Micro's Apex One and OfficeScan XG** enterprise security products.
3. In 2019 and 2020, the US Justice Department indicted five members of the Chinese APT known as APT41 with an intrusion campaign affecting more than 100 companies globally. APT41 compromised **software providers** and then modified the providers' code to facilitate further intrusions against the software providers' customers. The objectives of the campaign were espionage and cryptocurrency mining.
4. In October 2019, **Avast** announced a second breach of the CCleaner software. This time, the hackers successfully breached the infrastructure to which CCleaner hosting had been moved following the 2017 compromise. The Czech Security Information Service (BIS) attributed this attack to Chinese threat actors.
5. In October 2020, Google's Threat Analysis Group reported that Chinese state-sponsored hacking group APT31 impersonated the antivirus company McAfee to conduct targeted attacks on the Biden campaign's email system. Targets were prompted to install a legitimate version of **McAfee Total Protection** antivirus software from GitHub, while the malware was simultaneously installed to the system. **McAfee Total Protection is one of the antivirus packages purchased by Unit 61419 a year prior.**
6. In 2021, Microsoft announced that a Chinese state-sponsored hacking group, HAFNIUM, used four zero-day exploits to gain access to and install web shells on **Microsoft Exchange** servers, compromising Outlook Web Access (OWA) in as many as 60,000 organizations worldwide.

Additionally, **the Chinese government has not used foreign antivirus software for legitimate purposes since 2014, when it was banned.** In August 2014, the state-owned

news agency People's Daily reported that the Central Government Procurement Department (中央政府采购部门) excluded Kaspersky and Symantec from a list of approved information security software providers. Chinese officials approved the use of five China-based firms: Qihoo 360 Technology, Venustech, CAJinchen, Beijing Jiangmin, and Rising. China's Ministry of Public Security issued a notice in June 2014 stating that Symantec software had security vulnerabilities including backdoors that could allow outside access.

Who Is PLA Unit 61419?

Unit 61419 is the Military Unit Cover Designator (MUCD) for a bureau within the People's Liberation Army (PLA) Strategic Support Force (SSF). Although publicly available documentation is scarce, the unit's area of responsibilities included interpretation of foreign signals intelligence (SIGINT) and other cyber operations, with a focus on Japan and Korea, when it was first identified in 2011. Researchers at the Project 2049 Institute assessed Unit 61419 to be the 4th Operational Bureau of the PLA General Staff Department's (GSD) Third Department (3PLA). 3PLA was broadly responsible for defensive SIGINT, including monitoring Chinese communication networks, protecting the security of Chinese domestic computer networks, and conducting cyber espionage-oriented computer network exploitation (CNE). Beginning in 2015, the GSD and 3PLA were disbanded, with their capabilities and focus reorganized, at least in part, into the SSF's Network Systems Department (NSD). The unit is headquartered in Qingdao (location described in detail below) and comprises multiple subordinate offices, each with its own MUCD. These offices are located in Qingdao and surrounding areas, Hangzhou, Beijing, and Shanghai. Each of these offices likely has its own MUCD.[1] One of these, Unit 61680, is located in the Wenquan township (温泉镇) under Jimo city (即墨市) and has a training center there. Unit 61650 uses the same address as Unit 61419 for its equipment procurement, suggesting it is a subordinate office as well. Unit 61789 is subordinate as well and is probably located in Shanghai. Research conducted by Unit 61419 members includes a 2008 paper on the extension of the US's "nuclear umbrella" to Korea as well as medical topics, the latter focus suggesting the unit has a medical department. A logistics department manages Unit 61419's properties and a political department handles discipline and political education, as in most other PLA units. Unit 61419 may have a training base in Xinzhou, Shanxi province.[2]

***Figure 2**: Emblem of the People's Liberation Army Strategic Support Force*

Recent reporting from Japan implicates Unit 61419 in a series of cyberattacks on companies like Mitsubishi Electric, Hitachi, Keio University, Hitotsubashi University, and the Japan Aerospace Exploration Agency (JAXA) in 2016 and 2017. The wife of a member of Unit 61619 reportedly instructed a Chinese student living in Japan to rent servers using an alias. Those servers were then used in some of the cyberattacks referenced above. Japanese media further cited Japan's Tokyo Metro Police Department's Public Safety Bureau in asserting that Unit 61419 is linked to the Tick Group APT, which was also identified as being behind the 2016 and 2017 cyberattacks. Although definitive attribution of Tick Group to Unit

61419 remains difficult to confirm at this time, the APT has historically focused on Japanese targets. This aligns with Unit 61419's focus on Japan. Moreover, Tick Group's exploitation of zero-days impacting Trend Micro's Apex One and OfficeScan XG enterprise security products occurred months before a November 2019 procurement announcement for Trend Micro's Worry-Free Services Advanced was issued by an SSF unit using Unit 61419's headquarters as the application delivery address.
Given the tentative links to cyberattacks in Japan and Tick Group, as well as the procurement activities identified in this report, Unit 61419 most likely continues to operate as an SSF NSD bureau focused at least in part on CNE operations.

Locating Unit 61419

Insikt Group identified several important patterns from the six procurement documents. All six documents list a consistent point of contact — a "Mr. Yu" (于先生) — along with a phone number.
Six of the documents also list the same contact address in Qingdao City, Shandong province: No. 5 Fushun Road, Shibei District, Qingdao City, Shandong Province, postal code 266034 (山东省青岛市市北区抚顺路5号, 邮编266034), as seen in Figure 5, below. All of the procurement documents for Unit 61419 use this address. This address is also used for other units, such as 61650, that are likely subordinate to Unit 61419.

Figure 3: *Screenshot of address from procurement document application instructions*

In addition to the procurement documents, Insikt Group found a 2018 electricity outage notice listing Unit 61419's logistics department as an affected party on Fushun Road. The notice, in Figure 4 reads, "35kV Fushun Road Substation | Planned blackout … 61419 logistics department of the Army affects 2 stations and 231 district customers." ***Figure 4:*** *2018 electric outage notice identifies the Fushun Road substation as the power source for a facility managed by PLA's Unit 61419 Logistics Department*
Baidu Maps shows that No. 5 Fushun Road is the location of a hotel in Qingdao called the Bihaiyuan Hotel (碧海园宾馆). Some of the procurement documents No. 5 Fushun Road refer directly to this hotel or its front desk (Figure 7).

Figure 5: *Street view of Bihaiyuan Hotel (碧海园宾馆)* ***Figure 6:*** *Street view of Bihaiyuan Hotel (碧海园宾馆) and adjacent security checkpoint and gate* ***Figure 7:*** *Procurement footnotes direct the delivery of application materials to an address of the Bihaiyuan Hotel (碧海园宾馆)*
Recorded Future assesses that the No. 5 Fushun Road address is the headquarters of Unit 61419 and that the Bihaiyuan Hotel is its public face. Behind the hotel is a walled compound similar to the headquarters of other PLA units (Figure 8). Our assessment corroborates Project 2049 Institute's finding in 2011 that this address was the likely headquarters.

Figure 8: *Map of Bureau 61419's compound based on Insikt Group's analysis. The primary compound (shown in red) is adjacent to or shares space with two other gated facilities*

(shown in dark red). The degree to which the Unit 61419 compound is separated, as well as the level of security at internal gates, is unclear based on available satellite imagery.
For example, in a January 2016 report compiled by the US Army's Asian Studies Detachment, the Jingtang Hotel and Seasons Hotel were linked to the 4th Department of the General Staff Headquarters of the PLA (4PLA), which was responsible for electronic and information warfare, including offensive cyber operations, prior to its dissolution and reorganization into the SSF.

Limited evidence suggests the use of hotels is a model used by PLA units in a possible attempt to obfuscate their locations. Past reports have alleged that PLAY cyber and electronics units have leased floors of hotel rooms for their operations or as possible headquarters.

The Bihaiyuan Hotel is also not the only hotel associated with Unit 61419. A 2018 lawsuit filed by PLA Unit 61789 against Shanghai Golden Hope Hotel Management Co. Ltd. (上海金色希望酒店管理有限公司) over a breach of its "Military Real Estate Lease Contract", indicates that in 2014 Unit 61419 leased a building on Yan'an Middle Road in Shanghai to the hotel management company. The lawsuit indicates that Unit 61789 was subordinate to Unit 61419 in 2017. Unit 61850, former 3PLA's 7th Operational Bureau, is also identified as a party in the dispute. The location of the leased building may have been No. 802 Yan'an Middle Road, Jing'an District, Shanghai City, where Shanghai Golden Hope Hotel previously operated a hotel.

Recommendations

Given the pattern of Chinese state-sponsored exploitation of the global software supply chain described above, as well as China's exclusion of foreign antivirus software as an option for government organizations, the brands and products indicated in Table 1 should be monitored for future exploitation. Focus should be placed on adversarial simulations, penetration testing, patching known vulnerabilities, and monitoring for anomalous traffic related to these antivirus products.
While Recorded Future is not in a position to evaluate the precise legality of any transactions that may have resulted from the procurement documents we reviewed, we further recommend any impacted organization seek legal counsel about the sales of security software to China given the US Department of Commerce's Export Administration Regulations (EAR) regulations that cover information security software.

[1] Mark Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press: New York, NY, 2015, p. 171. [2] Ibid.