

HOW TO RECOGNIZE CHINA CYBER THREATS



HOW TO RECOGNIZE CHINA CYBER THREATS

Table of Contents

01 PREFACE 4
02 LIST OF ACRONYMS 5
03 INTRODUCTION 7
03.1. Context and Objectives of the Project 7
03.2. Approach and Methodology 7
03.3. Proposed Structure of the Guidebook 8
04 EXECUTIVE SUMMARY 9
05 CHINA'S CYBER DOCTRINE AND STRUCTURE 10
06 LIST OF THE MOST ACTIVE APTS ATTRIBUTED TO CHINA 13
6.1 APT27 13
6.1.1 Examples of Attacks and Data Compromise Attributed to APT27 14
6.1.2 Notable Attacks Linked to APT27: 14
6.2 APT40 15
6.2.1 Examples of Attacks and Data Compromise Attributed to APT40 16
6.2.2 Notable Attacks Linked to APT40: 16
6.3 APT41 17
6.3.1 Examples of Attacks and Data Compromise Attributed to APT41 18
6.3.2 Notable Attacks linked to APT41 18
07 TOOLS AND METHODS OF CHINESE CYBER OPERATIONS 20
08 RECOMMENDATIONS FOR DETECTION AND MITIGATIONS 21
09 COMPARISON WITH THE OTHER BIG 4 CYBER THREAT COUNTRIES 28
10 ENDING NOTES 32
ANNEX 1. List of China-attributed APTs from attack.mitre.org 33
ANNEX 2. North Korea's Most Used TTP's from attack.mitre.org 42
ANNEX 3. Iran's Most Used TTP's from attack.mitre.org 43
ANNEX 4. Russia's Most Used TTP's from attack.mitre.org 45
ANNEX 5. China's Most Used TTP's from attack.mitre.org 49

01/Preface

The People's Republic of China (PRC) is steadily gaining ground as the primary source of malicious cyber activity. Ranging from Distributed Denial-of-Service (DDoS) and phishing campaigns to malware and ransomware, China is the second-largest economy in the world, and it is becoming a significant threat in the global cyber domain. China's rapid economic growth and technological advancement have been mirrored in the country's cyber capability development. With an increased emphasis on digital transformation, China's cyber capabilities have emerged as a critical component in its national security and global influence strategy. The Regional Cyber Defence Centre (RCDC), a subdivision of the National Cyber Security Centre (NCSC) under the Ministry of National Defence of Lithuania, has developed a guidebook How to Recognize Chinese Cyber Threats which aims to compare China-based cyber threats to other state-sponsored Advanced Persistent Threats (APT) through the perspective of their used MITRE ATT&CK Tactics, Techniques and Procedures, targets, goals and malware used to achieve said goals. The guidebook was developed by the RCDC Cyber Threat Analysis Cell (CTAC) team and the rotating personnel from Ukraine, Georgia, the United States of America.

The overall objective of the Project is to develop a guidebook on How to Recognize China Cyber Threats that covers the most active Chinese APT groups and common cyber threats originating from China, ranging from ransomware, data exfiltration, and industrial espionage, all the way to supply chain attacks and compromised hardware, and to provide mitigating techniques and tactics, techniques, and procedures (TTP's) against China's threat actors.

02/List of acronyms

Table 1. List of acronyms

Term/abbreviation	Meaning/explanation
API	Application Programming Interface
APT	Advanced Persistent Threat
ASEAN	The Association of Southeast Asian Nations
BfV	The German Domestic Intelligence Services (German: Bundesamt für Verfassungsschutz)
BIG 4	China, Russia, Iran, and North Korea
C2	Command and Control
CCP	The Chinese Communist Party
CI	Continuous Integration
CD	Continuous Development
CTAC	The Cyber Threat Analysis Cell
DDoS	Distributed Denial of Service
DLL	Dynamic-link Library
ENISA	The European Union Agency for Cybersecurity
GDP	Gross Domestic Product
GSD	The General Staff Department
IDS	Intrusion Detection System
MITRE ATT&CK Framework	A curated knowledge base which tracks cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle
MITRE D3FEND Framework	Library of defensive cybersecurity countermeasures, technical components, and their associations and capabilities
MSS	The Ministry of State Security
MPS	The Ministry of Public Security
MUCD	Military Unit Cover Designator
NGO	Non-Governmental Organisation
PII	Personal Identifiable Information
PLA	The People's Liberation Army
PRC	The People's Republic of China
PLAGF	The People's Liberation Army Ground Force

Term/abbreviation	Meaning/explanation
RAT	Remote Access Trojan
RCDC	Regional Cyber Defence Centre
SQL	Structured Query Language
SOC	Security Operation Center
TTP	Tactics, Techniques, and Procedures
UNDP	The United Nations Development Programme
YAML	YAML Ain't Markup Language™

03/Introduction

3.1/Context of the Project

Established as a joint initiative of Lithuania and the United States, the RCDC aims to fill the niche of practical cooperation in the field of cyber defence and to strengthen the capacity of Lithuania and the regional partners to ensure cyber security of their states. One of the main RCDC goals is to become a regional platform for practical cooperation to help protect critical infrastructure from cyber attacks. To achieve this objective, RCDC activities are centred on strengthening the resilience and cyber defence capacity of public critical service providers.

3.2/Approach and Methodology

To achieve the Project objective, the following components constitute the development of the guidebook How to Recognize China Cyber Threats:

- Discussion on study goals and objectives.
- Collection of input and information from RCDC members and like-minded partners.
- Collection of information from commercial and publicly available sources.
- Collaborative processing, systemizing, and evaluating collected information with RCDC rotating personnel and partners remotely.
- Employment of various commercial and open-source tools for analysis, structuring, and processing of data.
- Cooperation with countries from the Asia-Pacific region.

The listed research activities were aimed to culminate in the How to Recognize China Cyber Threats guidebook which provides a systemic analysis of the most active Chinese advanced persistent threats (APTs) and their TTP's, compared to the other BIG 4 activities. The guidebook also offers detection and mitigation techniques that can be used inside of organisations.

3.3/Proposed Structure of the Guidebook

The guidebook is divided into the following parts:

- Section 4 is the Executive Summary;
- Section 5 briefly introduces China's cyber doctrine and structure;
- Section 6 lists the most active APTs attributed to China;
- Section 7 talks about tools and methods used by China;
- Section 8 proposes recommendations on detection and mitigation;
- Section 9 offers a comparison of it with other BIG 4 cyber threat countries;
- Section 10 is the conclusion;
- Annex 1. List of Chinese-attributed APTs from attack.mitre.org;
- Annex 2. North Korea's most used TTP's from attack.mitre.org;
- Annex 3. Iran's most used TTP's from attack.mitre.org;
- Annex 4. Russia's most used TTP's from attack.mitre.org;
- Annex 5. China's most used TTP's from attack.mitre.org.

04/Executive Summary

China has emerged as a prominent player in the global cyber landscape, exhibiting both state-sponsored and non-state cyber activities. The Chinese Government's cyber capabilities, coupled with its focus on economic and technological development, present significant risks to international security and economic interests.

State-sponsored cyber espionage campaigns attributed to China continue to target governments, corporations, and organisations worldwide. These campaigns aim to acquire sensitive information, intellectual property, and trade secrets to enable China to gain a competitive advantage across various industries.

China-attributed cyber threat actors employ a range of tactics, such as spear-phishing, malware deployment, supply chain attacks, and network exploitation, to name but a few. APTs linked to Chinese hacking groups, such as APT10 and APT41, have displayed sophisticated techniques and persistent targeting.

Critical infrastructure sectors, including energy, telecommunications, and finance, are at a particular risk posed by China's cyber activities. A potential disruption or compromise of said sectors can have severe economic and societal consequences, as witnessed in the previous cyber incidents attributed to China's threat actors.

As China's cyber capabilities expand, personal data theft poses a significant concern. Stolen data can be exploited for various purposes, including intelligence gathering, economic espionage, and influence operations. It raises privacy, national security concerns, as well as about the potential of targeting individuals or organisations with coercion or blackmail.

Addressing China cyber threat requires a comprehensive and multi-faceted approach: it is vital to adopt enhanced cybersecurity measures, including robust network defences, threat intelligence sharing, and incident response capabilities, to mitigate the risks. A close collaboration between governments, the private sector and international organisations is necessary to ensure norms are developed, best practices are shared, and malicious cyber activities are deterred.

Given the evolving nature of China's cyber capabilities, continued monitoring, research, and investment in cybersecurity are crucial. Organisations and governments must remain vigilant, enhance their cyber defenses, and adapt to the ever-changing threat landscape shaped by China's cyber activities.

05/China's Cyber Doctrine and Structure

According to the Constitution of the People's Republic of China and a set of regulations, the Communist Party of China (CPC) is the sole ruling party of the People's Republic of China (PRC).

The Central Military Commission (CMC) of the Communist Party of China is the highest national defence organisation which heads the People's Liberation Army (PLA), the People's Armed Police (PAP), and the Militia of China.

The PLA is the principal military force of the PRC and the armed wing of the CPC which has the Joint Staff Department (JSD) of the CMC as the command organ and the Headquarters. The PLA consists of five service branches: the Ground Force, Navy, Air Force, Rocket Force, and the Strategic Support Force (SSF, also called PLASSF).[1]

The PLASSF is a space, cyber, political, and electronic warfare force[2] whose mission is to improve the army's success in what China calls "informationized conflicts" and to enhance the PLA's power projection capabilities across space and cyberspace. This new force is purportedly designed to break stovepipes in the intelligence sharing and coordination departments of the different branches and to oversee all units responsible for psychological warfare, information warfare, space warfare, cyberwarfare, and electronic warfare operations. It is believed to have at least 5 departments: General Staff Department, Political Work Department, Disciplinary Inspection Commission, Space Systems Department, and the Network System Department (NSD). The NSD is an integration of all PLA information and cyberwarfare capabilities responsible for China's military computer network operations (CNO), signals intelligence (SIGINT) operations, offensive electronic warfare (EW) operations, information warfare (IW) missions, and offensive cyber operations. The NSD consists of 12 bureaus and 2 research institutes. The Intelligence Bureau of the JSD is one of the PLA's primary intelligence organisations and the principal military intelligence organ of the PLA that is responsible for strategic intelligence collection and analysis, primarily in clandestine human intelligence (HUMINT) operations. Although other intelligence disciplines (including cyber operations) have likely moved to the PLASSF, the Intelligence Bureau is still able to process information retrieved via cyberwarfare operations.

In addition to the military branch of the Communist Party of China, the executive branch of the CPC is also involved in conducting cyber operations. This branch is managed by the State Council of the People's Republic of China – the chief administrative authority of the PRC, chaired by the premier, and includes the heads of each of the constituent departments (ministries). Two involved ministries are the Ministry of Public Security (MPS) and the Ministry of State Security (MSS).

[1] https://www.britannica.com/topic/Chinese-Communist-Party

[2] https://jamestown.org/program/strategic-support-force-update-overview/

The MPS is a government ministry of the PRC responsible for public and political security. The creation of the MSS in July 1983 created the illusion that the MPS is simply a law enforcement police body, separate from intelligence agencies. However, according to Alex Joske, an independent analyst who worked at the International Cyber Policy Centre of the Australian Strategic Policy Institute[3], the MPS lost much of its foreign intelligence remit after the MSS's creation but has established new units for cross-border clandestine operations since then. The MSS[4] is the principal civilian intelligence, security, and secret police agency of the PRC, responsible for non-military foreign intelligence, counterintelligence, political, and domestic security. It consists of its primary central office, provincial departments, and several local and municipal bureaus. The MSS is active in industrial, economic, and cyber espionage. Since 2012, the MSS has gained more responsibility over cyber espionage with the PLA, and has sponsored various APT groups, such as Double Dragon (also known as APT41) and Leviathan (also known as APT40).

Summing up, the Chinese have one organisation responsible for counterintelligence (including cyber) inside the country – the Ministry of Public Services (MPS), and three main organisations/units allowed to carry out offensive cyber operations abroad:

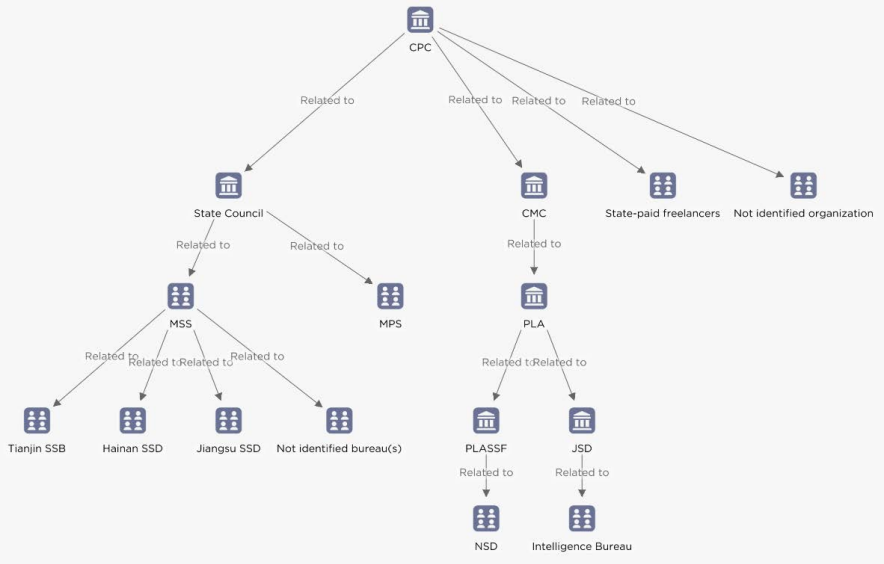
- The Network Systems Department (NSD),
- The Joint Staff Department (JSD),
- The Ministry of State Security (MSS).

Also, there are state-sponsored APT groups in China (probably sponsored by MPS) which also are involved in cyber operations of different levels.

[3] https://sinopsis.cz/wp-content/uploads/2022/01/mps0.pdf

[4] https://nationalinterest.org/feature/everything-we-know-about-chinas-secretive-state-security-21459

Figure 1. An approximate Chinese cyber structure (RCDC)



In 2023, Armis provided an estimated range of China's "hacker army" personnel, anywhere from 50,000 and more individuals[5]. It is very important to note that in China, there is a very large number of independent, financially motivated APT groups. These usually have some connection with the Government and the PLA but are allowed to operate independently for financial gain. Their tactics and procedures usually employ ransomware and data extortion to gain financial benefit in cryptocurrency form. The groups also prey on trade secrets of the private sector and engage in industrial espionage.

[5] https://www.armis.com/blog/the-cyberwarfare-capabilities-of-east-vs-west/

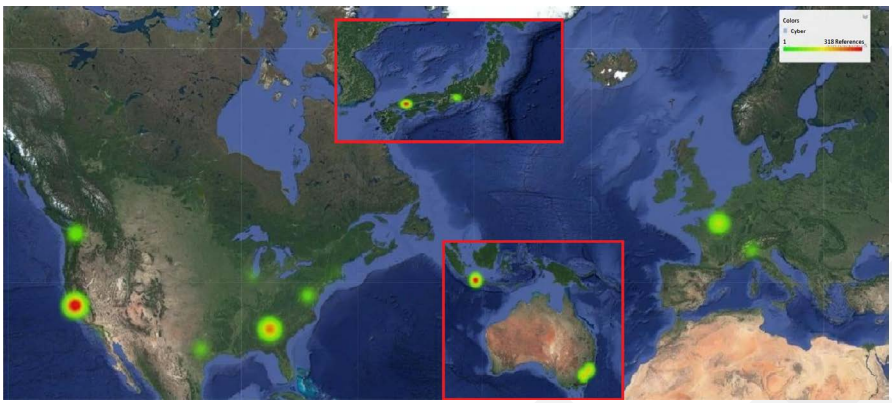
06/List of the Most Active APT's Attributed to China

The next section provides the list of the most active APT groups attributed to China, as well as the most notable attacks they have carried out.

6.1/APT27

APT27 (aka: GreedyTaotie, TG-3390, EMISSARY PANDA, TEMP.Hippo, Red Phoenix, Budworm, Group 35, ZipToken, Iron Tiger, BRONZE UNION, Lucky Mouse, G0027, Iron Taurus) has targeted numerous companies with headquarters in the Middle East, North and South America, Europe, and other parts of the world. The affected companies operate in a variety of sectors, including business services, high technology, government, and energy. However, a sizable portion of them is in aerospace, transportation, or travel sectors. APT27 conducts cyber operations to steal intellectual property, typically concentrating on the information and initiatives that make a specific organisation successful in its industry. Spear phishing is frequently used by APT27 as its initial method of compromise. Although APT27 threat actors do not typically use original zero-day exploits, they might once they are made public. At least once, APT27 actors have sent spear phishing emails to other victims in related industries using a compromised account of one victim organisation. APT27 is also likely to compromise weak web applications to establish a foothold.

Figure 2. APT27-most targeted countries.



6.1.1/Examples of Attacks and Data Compromise Attributed to APT27

APT27: Previously, APT27 has been accused of spying on 5 major telecommunication providers from Southeast Asia, Israeli organisations, and a US state legislature, among other targets. In 2020, the group started including ransomware-based cybercriminal activities in their operations. To gain an initial foothold, APT27 primarily relies on watering hole and spear phishing attacks, ENISA notes.

6.1.2/Notable Attacks Linked to APT27:

- February 2015 - Anthem health insurance provider, U.S., disclosed it had fallen victim to data breach which got personally identifiable information (PII) of 78.8 million people stolen. The post-breach analysis revealed the initial access vector was a phishing email sent to an employee a year prior. According to the same report, the breach resulted in Anthem spending $260 million to fix security-related issues and an additional $39 million to settle lawsuits from affected victims. Although this attack was never directly attributed to a nation-state, the presence of several APT27 TTP's (including C2 infrastructure and software), made the group the most likely culprit.

- March 2018 - APT27 compromised the national data centre of a Central Asian country. While present in the victim network since at least 4 months ago, the threat group used its official websites to run a watering hole attack. Users who interacted with malicious links hosted on the websites were redirected to APT27-controlled domains and downloaded ScanBox and BeEF frameworks to their systems without realising. The APT27 tool HyperBro was found on several systems inside the targeted environment.

- March 2021 - The BfV German Domestic Intelligence Services released a report alerting about APT27 attacks against German commercial organisations. In the documented attacks, APT27 exploited vulnerabilities in Zoho AdSelfService Plus software, a self-service password management tool, to gain the initial access. Once on the network, the threat group conducted espionage activity by leveraging legitimate software vulnerable to DLL side-loading to load HyperBro RAT in memory.

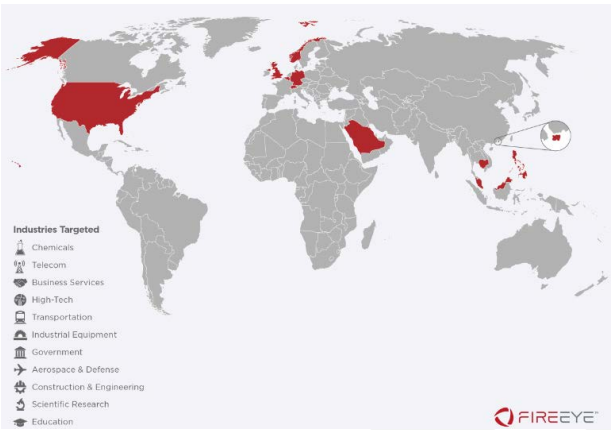
- April 2022 - Campaigns against a Middle Eastern government, an electronics manufacturer, a U.S. state legislature, and a Southeast Asian hospital over the month were all attributed to APT27. In these attacks, advantage was taken of the Log4j vulnerabilities to install web shells on web servers. Again, APT27 deployed its HyperBro RAT by dropping a copy of legitimate software (using CyberArk Viewfinity in the mentioned attacks) on victim systems and DLL side-loading the payload in memory.

- August 2022 - During the visit of the Speaker of the US House of Representatives Nancy Pelosi to Taiwan, an unknown organisation suspected of pretending to be APT27 released an online special operations video on YouTube on August 3 claiming that Taiwan was a Chinese territory and threatened to attack Taiwan's critical infrastructure. Another video followed on August 7 in which the threat actor claimed to have obtained access to over 200,000 devices, attacked the Department of Ministry of the Interior, the Highway Administrations and Taipower, and announced zero-day vulnerabilities of equipment manufacturers in Taiwan. In addition, a TV set was hacked in Taiwan's convenience store and played a video opposing the Nancy Pelosi visit to Taiwan. According to the public intelligence, it may have been possible because the TV set included China-made software.

6.2/APT40

APT40 (aka: TEMP.Periscope, TEMP.Jumper, Leviathan, BRONZE MOHAWK, GADOLINIUM, KRYPTONITE PANDA, G0065, ATK29, TA423, Red Ladon, ITG09, MUDCARP) frequently targets nations that are crucial to the Belt and Road Initiative from a strategic standpoint. Despite targeting international organisations, particularly those with an emphasis on engineering and defence, the group has also in the past Figure 3. waged campaigns against local organisations in places like Southeast Asia.

Figure 3. Countries and industries targeted by APT40, (FireEye)



Since at least January 2013, the group has launched campaigns against a variety of subjects, including maritime targets, defence, aviation, chemicals, research/education, government, and technology organisations. China's efforts to update its naval capabilities are mirrored in APT40's operations, which also include targeting extensive university research projects and obtaining blueprints for marine machinery and vehicles. To carry out their operations, the group frequent-

ly targets government-sponsored projects and steals significant amounts of information related to them, including proposals, meetings, financial data, shipping data, plans and drawings, and raw data. When sending spear-phishing emails, APT40 frequently assumes the identity of a well-known individual whom the target is likely to find interesting. This includes posing as a journalist, a representative of a trade publication, a member of an appropriate military organisation, or an official from a relevant non-governmental organisation (NGO). The group has occasionally sent spear-phishing emails using previously compromised email addresses.

6.2.1/Examples of Attack and Compromise of Data Attributed APT40

APT40: has historically targeted a wide range of industries including defence and government organisations, engineering firms, shipping and transportation, manufacturing, and research universities in the United States, Western Europe, Australia, and the South China Sea. The group has shown interest in maritime technology and countries strategically important to China's Belt and Road initiative. APT40 has been observed using a mixture of open-source and custom malware, including several custom tools shared across multiple Chinese state-sponsored groups, such as the JavaScript-based web reconnaissance and exploitation framework ScanBox. Open-source tools used by APT40 include Cobalt Strike Beacon, PowerShell Empire, Meterpreter, and Mimikatz.

6.2.2/Notable Attacks Linked to APT40:

Researchers at security company Proofpoint and PricewaterhouseCoopers (PWC) said on August 30, 2022, they had identified a cyber espionage campaign that delivers the ScanBox exploitation framework through a malicious fake Australian news site.[6] The campaign, active from April to June of 2022, targeted Australian Government agencies, Australian media companies, and manufacturers who conduct maintenance of wind turbine fleets in the South China Sea. Proofpoint said the victim profile was similar to a June 2021 TA423 (APT40) threat that delivered a downloader in DLL format via RTF template injection.

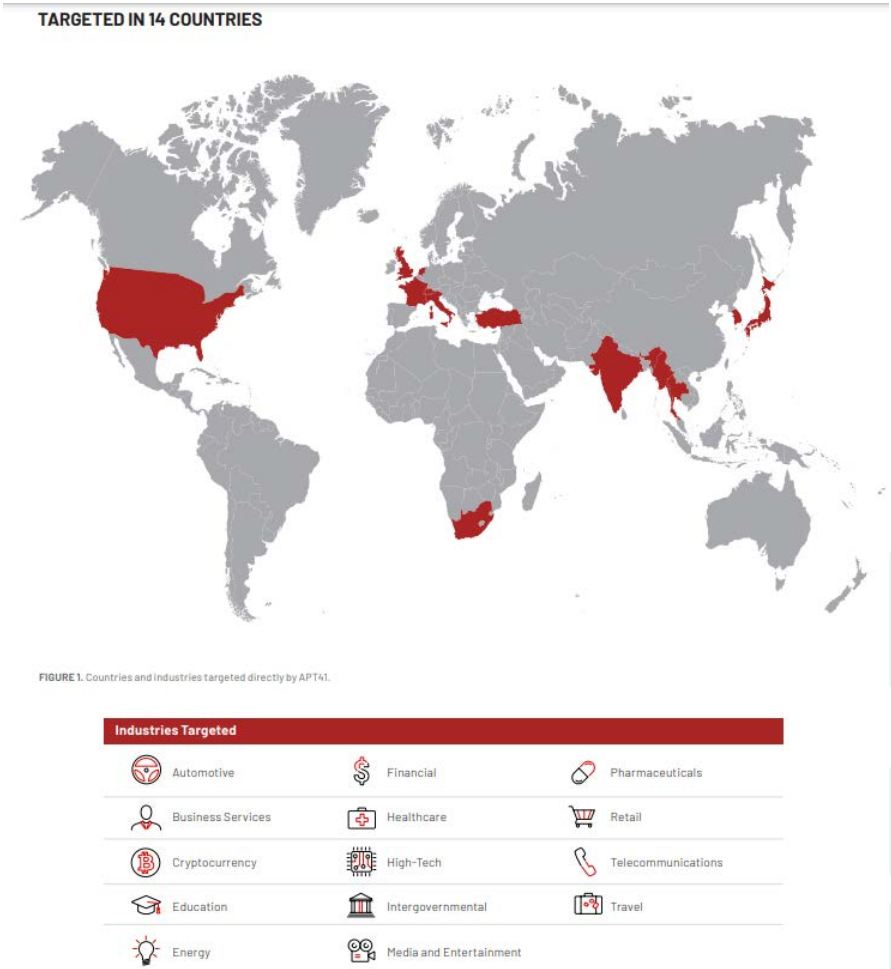
In 2020, the Taiwanese Government claimed that hackers with ties to the Chinese Government attacked 6,000 official email accounts, as well as 10 Taiwanese Government agencies, in an uptick in Beijing's long-running espionage on the island. Chinese hackers had infiltrated several Taiwanese Government offices over two years to steal sensitive documents.

[6] https://www.proofpoint.com/uk/blog/threat-insight/chasing-currents-espionage-south-china-sea

6.3/APT41

APT41 (aka: G0096, TA415, Blackfly, Grayfly, LEAD, BARIUM, WICKED SPIDER, WICKED PANDA, BRONZE ATLAS, BRONZE EXPORT, Red Kelpie, G0044, Earth Baku, Amoeba) is a well-known cyber threat group that engages in financially motivated activity that may not be controlled by the Figure 4. Government, as well as state-sponsored espionage on behalf of the Chinese Government.

Figure 4. Countries and industries targeted directly by APT41 (Mandiant)



Since at least 2012, APT41 has targeted businesses in at least 14 different nations. The group has historically stolen intellectual property as part of its espionage campaigns which have targeted the high-tech, telecom, and healthcare industries. Their cybercrime intrusions targeting the video game industry include manipulation of virtual currencies and attempted ransomware deployment. Some evidence that APT41 also tracks people and conducts surveillance can be found in the group's operations against higher education institutions, travel agencies, news, and media companies. To initially compromise their victims, APT41 frequently uses spear-phishing emails with attachments like compiled HTML (.chm) files. Once inside a target organisation, APT41 can use more advanced TTP's and introduce new malware. For instance, throughout a nearly one-year campaign, APT41 infected hundreds of systems and employed almost 150 different types of malware, such as backdoors, credential stealers, keyloggers, and rootkits. To conceal its malware and maintain persistence on a small number of victim systems, APT41 has also deployed rootkits and Master Boot Record (MBR) bootkits.

6.3.1/Examples of Attack and Compromise of Data Attributed APT41

APT41: the group's campaigns for stealing intellectual property have historically included targeting the high-tech industry, telecoms, and the healthcare industry. Targeting the video game business, they have a history of cybercrime incursions, including attempted ransomware deployment and manipulation of virtual currencies. The organisation frequently uses spear-phishing, water holes, supply chain assaults, and backdoors to acquire network access to learn more about the targeted industry and collect information for upcoming attacks. There is evidence that the organisation has also engaged in code injection, file downloads, keylogging, screenshots, connecting to and accessing SQL databases, and clipboard data theft.

6.3.2/Notable Attacks Linked to APT41

- Between May 2021 and February 2022, two zero-day assaults targeted the USAHERDS app. According to the notice, "one CVE was accessed using a MachineKey and the other from Log4Shell."[7] Though the inquiry is still ongoing, state governments of at least six US states were infiltrated. There may be further unidentified victims.

- FireEye identified a campaign by APT41 (also known as BARIUM) in which the organisation tried to take advantage of flaws in Cisco routers, Citrix NetScaler/ADC, and Zoho ManageEngine Desktop Central. Targeted businesses in the financial, construction, defence, industrial, government healthcare, hi-tech, higher education, legal, manufacturing, media, transportation, travel, and utilities sectors were in the focus of the campaign which lasted from January 20, 2019,

[7] https://www.scmagazine.com/analysis/apt41-spear-phishing-supply-chain-campaigns-target-pharma-healthcare

through March 11, 2020. Attack victims have been reported from Australia, Canada, Denmark, Finland, France, Germany, Italy, Japan, Mexico, Philippines, Poland, Qatar, Saudi Arabia, Singapore, Sweden, Switzerland, United Arab Emirates, United Kingdom, and the United States. During the post-exploitation phase, the gang was observed using the trial version of the Cobalt Strike BEACON loader, a VMProtected Meterpreter downloader, and the Cobalt Strike BEACON shellcode.

- PaltoAlto researchers have detected a campaign in which the APT41 threat actor disseminated the Speculoos backdoor by taking advantage of the CVE-2019-19781 vulnerability. Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP equipment are all affected by the vulnerability, which enables remote command execution by an attacker. The assaults hit targets around the globe, including in North America, South America, and Europe, in the healthcare, higher education, manufacturing, government, and technology sectors.

07/Tools and Methods of Chinese Cyber Operations

The market for malware and tooling is robust across the Chinese cybercriminal underground. The Chinese-language cybercriminal underground has unique characteristics compared to other cybercriminal communities, such as the Russian-speaking cybercriminal underground. At the time this Report is released, no confirmed major ransomware-as-a-service (RaaS) or infostealer malware-as-a-service (MaaS) programs originate from China. Despite those omissions, various other malware and fraud-related tools are traded on Chinese-language dark web marketplaces and shared on Clearnet hacking forums. In addition, a rapidly growing domestic cybersecurity industry has produced more capable researchers. Proof-of-concept (POC) exploits for newly discovered vulnerabilities are frequently shared on personal blogs and repositories of researchers which cybercriminals could use. The development of homegrown penetration testing tools is also on the rise.

Malware families offered on Chinese-language dark web marketplaces are primarily tools to facilitate financially motivated cybercrime, such as remote access trojans (RATs) capable of stealing system information and account credentials. Botnets and DDoS services are also available. Some of the RATs (Gh0st RAT, PCShare) and web shells (China Chopper) advertised on Chinese-language dark web and Clearnet sources are also used by the Chinese state-sponsored threat activity groups, including RedFoxtrot, APT27, APT40, and APT41. Tools that facilitate phishing schemes are a fixture across the Chinese-language dark web ecosystem. There are a variety of phishing kits targeting global retailers and native payment applications, as well as cryptocurrency trading apps and platforms.

Supply Chain Cyber attack is another common cyber attack that is often related to China. A supply chain attack, a value-chain or third-party attack, occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data. This has dramatically changed the attack surface of the typical enterprise in the past few years, with more suppliers and service providers touching sensitive data than ever before. Most commonly, supply chain attacks come in two forms. Digital - when an organisation is exposed via compromised software they purchase and use, or their CI/CD process gets compromised. Physical - when an organisation purchases hardware and equipment that has been tampered with and has special components implanted for data exfiltration and malicious activity. Both of these are quite common, but physical more commonly originates from China, since more hardware and less software are produced and exported by China. POCs and sophisticated hacking tools are developed domestically and shared by Chinese researchers on Clearnet forums that have managed to survive Government crackdowns on cybercrime.

08/Recommendations for Detection and Mitigations

Detection

Detection of cyber threats in general is a complicated process. Tailoring a detection process to China-related cyber threats is even more complicated. Usually, attribution to a state or a state-sponsored actor can be done only after an extensive investigation and analysis of various indicators, tactics, patterns, and procedures. There are some options listed below that can be utilised as a starting point:

- Automated tools. The MITRE DeTT&CT framework allows to process various sources of information and look for specific patterns, TTP's, and indicators that could point to a possible attribution to China state or affiliated threat actors and their activity.
- Manual detection and review. A skilled cyber threat hunter can correlate IDS information and detect the emerging patterns indicating possible China-related malicious activity. However, this is time-consuming and expensive since it requires highly skilled cyber specialists.
- Commercial options. There is many commercial intelligence information and detection services available for monitoring China-related threat actors. These tools can provide intelligence, alerting, and general information related to cyber activity. Commercial solutions help solve the common problem which is that most Chinese threat actors target non-Chinese-speaking countries. Language barrier presents a big challenge in detection and defence. Commercial organisations often have Chinese-speaking staff and can process information much faster and with greater accuracy.

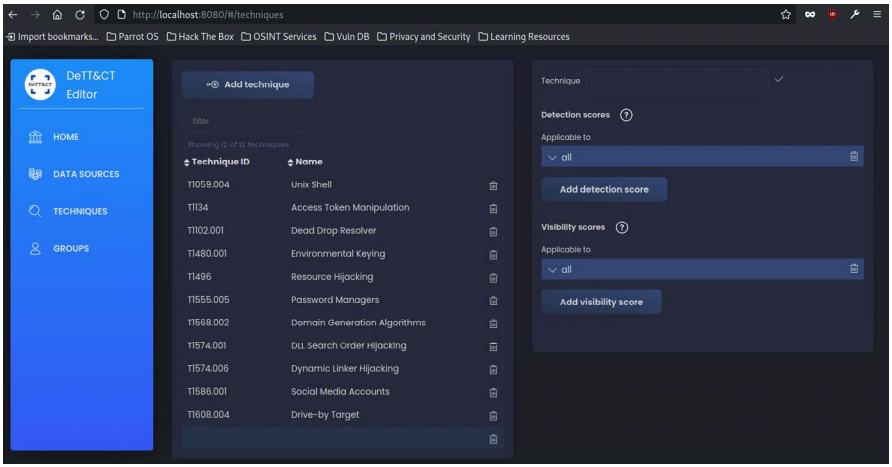
After comparing multiple TTP's, it is possible to see that the TTP's below are somewhat common to the China-based threat actors. These are not unique, but if these are detected in your system it might indicate that the attacker originates from China.

Table 3. (TTP's mainly used by China's APT groups)

TTP's mainly used by China's APT groups	
Code	Name
T1059.004	Command and Scripting Interpreter: Unix Shell.
T1102.001	WecanDead Drop Resolver.
T1134	Access Token Manipulation.
T1480.001	Execution Guardrails: Environmental Keying.
T1496	Resource Hijacking.
T1555.005	Credentials from Password Stores: Password Managers.
T1568.002	Dynamic Resolution: Domain Generation Algorithms.
T1574.001	Hijack Execution Flow: DLL Search Order Hijacking.
T1574.006	Hijack Execution Flow: Dynamic Linker Hijacking.
T1586.001	Compromise Accounts: Social Media Accounts.
T1608.004	Stage Capabilities: Drive-by Target.

The listed TTP's can then be imported into the MITRE DeTT&CT framework and connected to the data sources in your system like security information and event management (SIEM). This allows automatic detection of possible breaches in your environment.

Figure 5. Detect Tactics, Techniques & Combat Threats (DeTT&CT) graphical user interface



Building (Figure 5.) detection capabilities is a complex task, especially with a constantly increasing number of data sources. Keeping track of these data sources and their appropriate detection rules, or avoiding duplicate detection rules covering the same techniques, can give a hard time to detection engineers. For a security operations centre (SOC), it is crucial to have a good overview and a clear understanding of its actual visibility and detection coverage to identify gaps, prioritise the development of new detection rules, or onboard new data sources.

Mitigation

Mitigation of cyber risks emanating from China necessitates a proactive and comprehensive cybersecurity posture. Organisations should emphasise an ongoing risk assessment to discover vulnerabilities, strengthen their cyber hygiene practices with regular upgrades and robust authentications, and create a security-aware workforce through focused employee training. For containing possible breaches, network security techniques, such as segmentation and intrusion detection systems, are critical. Collaboration with peers in the industry, sharing threat intelligence, and applying geolocation filtering can provide useful insights and strengthen defence measures. Organisations can effectively manage the dangers posed by cyber threats from China by implementing a holistic strategy that incorporates technical protection, employee awareness, and collaboration.

These TTP's can be mitigated using the MITRE D3FEND matrix:

Table 4. Mitigation of Chinas mainly used TTP's using MITRE D3FEND

TTP's mainly used by China's APT groups		MITRE D3FEND
Code	Name	Mitigation techniques
T1059.004	Command and Scripting Interpreter: Unix Shell.	D3-EAL: Executable Allowlisting: Using a digital signature to authenticate a file before opening. D3-EDL: Executable Denylisting: Blocking the execution of files on a host following defined application policy rules.
T1102.001	WecanDead Drop Resolver.	D3-CSPP: Client-server Payload Profiling: Comparing client-server request and response payloads to a baseline profile to identify outliers. D3-PMAD: Protocol Metadata Anomaly Detection: Collecting network communication protocol metadata and identifying statistical outliers. D3-RTSD: Remote Terminal Session Detection: Detection of an unauthorised remote live terminal console session by examining network traffic to a network host. D3-UGLPA: User Geolocation Logon Pattern Analysis: Monitoring geolocation data of user logon attempts and comparing it to a baseline user behaviour profile to identify anomalies in logon location.

TTP's mainly used by China's APT groups		MITRE D3FEND
Code	Name	Mitigation techniques
T1134	Access Token Manipulation.	D3-CTS: Credential Transmission Scoping: Limiting the transmission of a credential to a scoped set of relying parties. D3-CRO: Credential Rotation: Expiring an existing set of credentials and reissuing a new valid set
T1480.001	Execution Guardrails: Environmental Keying.	No standardised D3FEND tactic exists yet. Other perimeter defence methods should be used to mitigate this threat.
T1496	Resource Hijacking.	No standardised D3FEND tactic exists yet. Other perimeter defence methods should be used to mitigate this threat.
T1555.005	Credentials from Password Stores: Password Managers.	D3-LFP: Local File Permissions: Restricting access to a local file by configuring operating system functionality. D3-FE: File Encryption: Encrypting a file using a cryptographic key.
T1568.002	Dynamic Resolution: Domain Generation Algorithms.	D3-NTF: Network Traffic Filtering: Restricting network traffic originating from any location. D3-DNSDL: DNS Denylisting: Blocking DNS Network Traffic based on criteria such as IP address, domain name, or DNS query type. D3-DNSAL: DNS Allowlisting: Permitting only approved domains and their subdomains to be resolved.
T1574.001	Hijack Execution Flow: DLL Search Order Hijacking.	D3-FA: File Analysis: File Analysis is an analytic process to determine a file's status. For example: virus, trojan, benign, malicious, trusted, unauthorised, sensitive, etc. D3-FE: File Encryption: Encrypting a file using a cryptographic key. D3-LFP: Local File Permissions: Restricting access to a local file by configuring operating system functionality.

TTP's mainly used by China's APT groups		MITRE D3FEND
Code	Name	Mitigation techniques
T1574.006	Hijack Execution Flow: Dynamic Linker Hijacking.	D3-FA: File Analysis: File Analysis is an analytic process to determine a file's status. For example: virus, trojan, benign, malicious, trusted, unauthorised, sensitive, etc. D3-FE: File Encryption: Encrypting a file using a cryptographic key. D3-LFP: Local File Permissions: Restricting access to a local file by configuring operating system functionality.
T1586.001	Compromise Accounts: Social Media Accounts.	No standardised D3FEND tactic exists yet. Other perimeter defence methods should be used to mitigate this threat.
T1608.004	Stage Capabilities: Drive-by Target.	No standardised D3FEND tactic exists yet. Other perimeter defence methods should be used to mitigate this threat.

09/Comparison with other BIG 4 Cyber Threat countries

The table below presents a classification and comparison of threat actors from the BIG 4 nations based on their unique goals, targets, and tactics, techniques, and procedures (TTP's) used in cyber operations. It distinguishes between various nation-states and cybercriminal organisations, emphasising their origins geographically, favoured targets (like governmental bodies, vital infrastructure, or financial institutions), general objectives (like espionage, profit, or disruption), and particular techniques used (like phishing, malware distribution, or network exploitation). Threat intelligence and cybersecurity defence strategies benefit from this comparative analysis because of the way it helps to comprehend the various tactics and modes of operation used by threat actors across various geopolitical boundaries.

Comparison with other BIG 4 Cyber Threat countries

Table 5. Comparison of BIG 4

China	North Korea	Iran	Russia
Related APTs: Summary			
The Chinese state-sponsored APT groups are known to have cutting-edge capabilities and target a variety of global businesses, institutions, and governments. These groups are notorious for their strategic focus, innovative techniques, and tenacious campaigns designed to steal confidential information, valuable data, and intellectual property.	The North Korean state-sponsored APT groups are notorious for their aggressive and unorthodox cyberespionage methods. These groups use cyberspace to further their military, financial, and political goals.	The Iran state-sponsored APT groups are known for their persistent and evolving tactics which target various industries and nations. These groups conduct strategic cyber operations to achieve political, military, and ideological objectives.	The Russian state-related APT groups seek governmental information retrieval, commonly using spearfish emails with the main module dropper delivered in a not-so-proficient attachment file.
Primary Goals			
China's cyber operations are often associated with espionage, intellectual property theft, and advancement of national interests in technology and industrial sectors.	North Korea's cyber activities are primarily driven by economic motives, focusing on generating revenue through hacking, including cryptocurrency theft and ransomware.	Iran's cyber activities aim to counter perceived threats, assert regional influence, and gather intelligence to support its geopolitical and security interests.	Russia's cyber operations are often linked to geopolitical objectives, including information warfare, political influence, and destabilisation efforts.
Main target countries/regions			
The United States Japan South Korea South East Asia Taiwan	The United States Japan South Korea India Malaysia Indonesia	The United States Middle East Israel	The United States Middle East Ukraine Europe
Initial access TTP's			
Spear Phishing, Watering Hole Attacks, Supply Chain Compromises, Malicious Documents, Zero-Day Exploits.	Drive-by Compromise, Spear Phishing Attachment, Zero-Day Exploits, Social Engineering, Watering Hole Attacks.	Spear Phishing, Credential Phishing, Remote Desktop Protocol (RDP) Exploitation, Web Shell Deployment, and Social Engineering.	Drive-by Compromise, Exploit Public-Facing Applications, External Remote Services, Spear Phishing Attachment, Compromise Software Supply Chain, Trusted Relationship.

China	North Korea	Iran	Russia
Used malware examples			
Virtualpita(-pie,-gate), Poison Ivy RAT, PlugX, Okrum, LowBall, ShadowPad, Winnti for Linux, ELMER, 9002 RAT, HiKit, ZXShell, ShadowPad, Spyder, Winnti, Red Charon, OwlProxy, Graphican, Sysget/HelloBridge, FormerFirstRat, NFlog, NewCT, Termite, MQsTTang, Angryrebel, Chinoxy, Trochilus RAT.	Maui, DTrack, EarlyRat, RokRAT, FadeStealer, RustBucket, ReconShark, OpenCarrot, ScoutEngine.	POWERSTAR and Core Impact backdoors, Nanocore RAT, Quasar RAT, Remcos, DarkComet, PlugX, MechaFlounder, ShellClient RAT, PupyRAT, TinyZbot, Woolger, Matryoshka RAT, TDTESS, LittleLooter, Liderc, Imecab, MimiKatz, Sorgu, POWERSTAR backdoor, BellaCiao, StrifeWater RAT, Saitama, PowerExchange.	Quarterrig, GraphicalNeutrino, GraphicalProton, Cheerscrypt, Night Sky, Rook, Pandora, Graphiron, Dridex, DoppelPaymer, WastedLocker, ServHelper, Octopus, RoarBat, Industroyer, TRISIS/TRITON, Capibar, Kazuar, DeliveryCheck, Diavol, BazarBackdoor, Anchor, BumbleBee.

Iranian APT groups

APT33: APT33 has targeted businesses with headquarters in the US, Saudi Arabia, and South Korea, spanning a variety of industries. Organisations involved in both military and commercial aviation and those in the energy sector with ties to petrochemical production have drawn particular attention from APT33.

APT34: This threat group has targeted numerous sectors, including the financial, government, energy, chemical, and telecommunications, and it has mainly concentrated its operations in the Middle East.

APT39: APT39's activities are primarily focused on the Middle East, despite its global targeting scope. APT39 has given the telecommunications sector priority, with additional focus on the travel sector, IT companies that support it, and the high-tech sector.

North Korean APT groups

Lazarus Group: A state-sponsored cyber threat organisation that has been linked to the Reconnaissance General Bureau. The group has used its abilities to target and compromise a variety of victims since 2009. Data was stolen in some intrusions, while other attacks have simply been disruptive. The group uses DDoS botnets, keyloggers, RATs, and wiper malware as tools and capabilities. Destover, Duuzer, and Hangman are other examples of the malware and tools that the group uses.

APT37: South Korea, Japan, Vietnam, and the Middle East are the main targets of this group: these markets are in a variety of industry verticals, such as chemicals, electronics, manufacturing, aerospace, automotive, and healthcare.

APT38: A state-sponsored threat group that specialises in financial cyber operations; it has been attributed to the Reconnaissance General Bureau. Active since at least 2014, APT38 has targeted banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries worldwide.

Russian APT groups

APT28: The group primarily targets nations and militaries in Eastern Europe, NATO, other European security organisations, and defence companies. It also targets the Caucasus, particularly Georgia.

APT29: A threat group that has been attributed to Russia's Foreign Intelligence Service (SVR) 17. They have operated since at least 2008, often targeting consulting, technology, telecom, and other organisations in North America, Europe, Asia, and the Middle East.

Sandworm: The threat group, attributed to GRU's unit 74455, has been active since at least 2009. In October 2020, the US indicted six GRU Unit 74455 officers associated with Sandworm Team for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and Government organisations, the 2017 worldwide NotPetya attack, targeting of the 2017 French presidential campaign, the 2018 Olympic Destroyer attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019.

The list of TTP's for each country (see the Annexes) reflects its unique focus and capabilities. For example:

- North Korea appears to focus on the techniques related to command and scripting interpreters (PowerShell, Windows Command Shell, Visual Basic), with an emphasis on different application layer protocols.
- Iran shows a mix of credential dumping, remote services, and exfiltration techniques, indicating a potential focus on data theft and compromise.
- Russia demonstrates a wide range of TTP's, including many related to credential dumping, discovery, and various execution methods.
- China seems to emphasise credential dumping, system service discovery, and remote services, with additional attention to techniques, like domain trust discovery and active scanning.

Some common TTP's appear across multiple countries, such as OS Credential Dumping, Remote Services usage (Remote Desktop Protocol, SMB/Windows Admin Shares), Scheduled Task/Job usage, Data from Local System, and System Network Configuration Discovery.

10/Ending notes

Recognizing cyber threats originating from China requires a comprehensive understanding of the modus operandi, tactics, and infrastructure commonly employed by the threat actors associated with the region. In this guidebook, a few several key indicators and strategies, helping identify potential cyber threats originating from China were covered:

- Attribution through Tactics, Techniques, and Procedures (TTP's): Studying and recognizing specific patterns of the attack methods, tools, and procedures can provide insights into the origin of a cyber threat. Chinese threat actors often have distinctive TTP's which, when identified, can suggest a connection to threat groups associated with China.

- Analysis of Targeted Sectors and Geographical Areas: Recognizing patterns in targeted sectors and regions can offer clues about the origin of the cyber threat. Threat actors affiliated with China might focus on sectors aligned with the country's strategic interests, such as technology, telecommunications, defence, finance, and government institutions. Geographical targeting, especially in Asia and regions connected to the Belt and Road Initiative, could be another indicator for attribution.

- Use of Specific Malware or Tools: Certain malware families or tools may be associated with threat groups from China. Monitoring and analysing the use of known malware strains or custom tools linked to Chinese threat actors can aid in identification.

- Language and Cultural Clues: Communication in Mandarin or use of Chinese cultural references in the code, metadata, or phishing lures might indicate an association with threat actors from China. Language analysis and cultural context could provide valuable clues during investigations.

- Infrastructure and Command-and-Control (C2) Servers: Identifying and tracking infrastructure, including IP addresses, domains, or servers used for command-and-control purposes, might reveal connections to previous cyber incidents linked to China.

- Historical Context and Political Motivations: Understanding the broader geopolitical landscape and historical context of cyber activities related to China can aid in recognizing potential threats. Political motivations and strategic goals can shape cyber operations.

Recognizing cyber threats are from China is a multifaceted process that requires continuous monitoring, analysis, and collaboration among cybersecurity professionals, researchers, and global stakeholders to effectively identify and mitigate potential risks and attacks.

China's ambitions to become a major technological and military force around the world are evident in the country's significant advancements in cyberspace. Since China places a strong emphasis on innovation and digital transformation, it is anticipated that its cyber activities will continue to develop, potentially changing the dynamics of global cybersecurity. To mitigate emerging cyber threats from China and other cyber actors, the global community must remain vigilant, promote international cooperation, and develop effective strategies.

Annex 1.

List of Chinese Attributed APTs from attack.mitre.org

Group Name	Description
APT1 (G0006, PLA Unit 61398, Comment_ Crew, Comment_Panda, GIF89a, Byzantine_ Candor, TG-8223)	Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. Belongs to PLA Unit 61398, and has cases that attacked Canada, France, Japan, Singapore, UK, US and Taiwan. Attack domain includes IT, aerospace, telecom, energy, transportation finance and government sectors.
APT2 (G0024, PLA Unit 61486, Putter_Panda, TG-6952)	Putter Panda was the subject of an extensive report by CrowdStrike. Putter Panda is sometimes referred to as "MSUpdater" by the security research community, this group has been operating since at least 2007 and has heavily targeted the US defence and European satellite/aerospace industries. They focus their exploits against popular productivity applications such as Adobe Reader and Microsoft Office to deploy custom malware through targeted email attacks. PUTTER PANDA has been observed conducting operations with a nexus to Shanghai, China, likely on behalf of the Chinese PLA 3rd Department 12th Bureau Unit 61486.
APT3 (G0022, Buckeye, UPS_Team, Pirpi, Gothic_Panda, TG-0110)	China-based threat group that researchers have attributed to China's Ministry of State Security (MSS). They have a history of using browser-based exploits as zero-days. As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organisations in Hong Kong. APT3's command and control (CnC) infrastructure is difficult to track, as there is little overlap across campaigns. Related to the Ministry of State Security, PRC. Earliest discovered in 2009, utilises remote access trojan to conduct attacks against US enterprises. Its target varies, which includes aerospace, defence, construction, energy, high-tech, non-profit organisations, telecom and transportation sectors.

Group Name	Description
APT5 (Pitty_Tiger, Pitty_Panda, Keyhole_Panda, Tabcteng, Manganese, Mulberry_Typhoon, Bronze_Fleetwood)	China-based threat group that has been active since 2007. APT5 targeted telecommunications companies and the network of an electronics firm that sells products for both industrial and military applications. The group subsequently stole communications related to the firm's business relationship with a national military, including inventories and memoranda about specific products they provided. In 2014 the APT5 made unauthorised code modifications to files in the embedded operating system of a technology platform. The group targeted mostly Southern Asian countries. According to the Microsoft Digital Defense Report (October 2021), the APT5 group was related to the exploitation of a 0-day exploit in a Pulse Connect Secure appliance. The Department of Homeland Security Cybersecurity and Infrastructure Security Agency released an alert on the same 0-day activity indicating that it affected US government agencies, critical infrastructure entities, and other private sector organisations likely beginning in June 2020. Related to the Ministry of State Security, PRC, previously focused targets on high-rech, telecom and SAT-COM domain to attack; intelligence shown since 2020, they utilise product vulnerabilities to VPN service providers to conduct supply chain attacks on government agencies in Europe and US, defence industry and finance institutes. Its target domains also consist of high-tech, telecom and SAT-COM.

Group Name	Description
APT10 (G0045, Red_Apollo, Menu-Pass, Stone_Panda, Potassium)	APT10 is a threat group that has been active since at least 2006. Individual members of APT10 are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company. APT10 has targeted healthcare, defence, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organisations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university. In April 2019 targeted government and private organisations in the Philippines. In 2020 Symantec implicated Red Apollo in a series of attacks on targets in Japan. In March 2021 they targeted Bharat Biotech and the Serum Institute of India, the world's largest vaccine maker's intellectual property for exfiltration. Related Monostry of Statew Security, PRC, the earliest activities can source back to 2006, the main targets are domains of PRC financial competitor companies, such as construction, engineering, aerospace and telecom. It's expanding to the medical and defence industry, finance, marine, energy, finance and government industries.
APT12 (G0005, IXESHE, DynCalc, Numbered_ Panda, DNSCALC)	Threat group that has been attributed to China and is believed to have been operating since 2009. Typically they target media outlets, high-tech companies, and governments in East Asia. One of the group's typical techniques is to send PDF files loaded with malware via spear phishing campaigns. The decoy documents are typically written in traditional Chinese, which is widely used in Taiwan, and the targets are largely associated with Taiwanese interests. This group has used multiple variants of DNS Calculation techniques.
APT15 (G0004, Nickel, Vixen_Panda, Nylon_ Typhoon, ke3chang, Mirage, Playful_Dragon)	Attributed to actors operating out of China, Ke3chang has targeted oil, government, diplomatic, military, and NGOs in Central and South America, the Caribbean, Europe, and North America since at least 2010.

Group Name	Description
APT16 (G0023, SVCMONDR)	A China-based group, active from at least 2015, launched several spear-phishing attacks targeting Japanese and Taiwanese organisations in the high-tech, government services, media, and financial services industries.
APT17 (G0025, Tailgator_Team, Deputy_Dog)	China-based threat group that has conducted network intrusions against the U.S. government, international law firms, and information technology companies. The threat group took advantage of the ability to create profiles and post in forums to embed encoded CnC for use with a variant of the malware it used. This technique can make it difficult for network security professionals to determine the true location of the CnC, and allow the CnC infrastructure to remain active for a longer period.
APT19 (G0073, Codoso_Team, Sunshop_Group)	Chinese-based threat group that has targeted a variety of industries, including defence, finance, energy, pharmaceutical, telecommunications, high-tech, education, manufacturing, and legal services. In the most recent versions, APT19 added an application whitelisting bypass to the XLSM documents. At least one observed phishing lure delivered a Cobalt Strike payload. Some analysts track APT19 and Deep Panda as the same group. According to Mandiant, this group is composed of freelancers with some degree of sponsorship by the Chinese government.
APT20 (Wacao, Twivy, th3bug)	Chinese-based threat group that has been active since 2009 and is known to rely on watering hole attacks. APT20 engages in cyber operations where the goal is data theft. APT20 conducts intellectual property theft but also appears interested in stealing data from or monitoring the activities of individuals with particular political interests. According to Mandiant, this group is composed of freelancers with some degree of sponsorship by the Chinese government.
APT22 (G0039, Suckfly, Barista)	Chinese-based threat group that has been operational since at least early 2014, carrying out intrusions and attack activity against public and private sector entities, including dissidents, and a set of political, military, and economic entities in East Asia, Europe, and the U.S. APT22 threat actors have used strategic web compromises in order to passively exploit targets of interest. APT22 actors have also identified vulnerable public-facing web servers on victim networks and uploaded web shells to gain access to the victim network.

Group Name	Description
APT26 (Deep_Panda, KungFu_Kittens, Black_Vine, Shell_Crew)	APT26 engages in cyber operations where the goal is intellectual property theft, usually focusing on the data and projects that make a particular organization competitive within its field. The group frequently uses strategic web compromises to gain access to target networks and custom backdoors once they are inside a victim environment.
APT27 (Emissary_Panda, Temp.Hippo, Red_Phoenix, Budworm, Group_35, Iron_Tiger, Lucky_Mouse, Bronze_Union, TG-3390)	Chinese-based threat group, active since at least 2010, that did one of the most famous false-flag efforts by use of a hacking tool previously associated with Iranian operatives, and embedded some of their malicious code with Farse, the predominant language in Iran. This led to Iran and Israel repeatedly blaming each other for continuous cyber attacks in 2018 and 2019. In December 2019, Iran's minister of information, communications, and technology blamed APT 27 — a suspected Chinese government-linked group — for a "cyberattack" on Iranian government networks.
APT30 (G0013, Lotus_Blossom, Radium, Raspberry_Typhoon)	APT30 is noted not only for sustained activity over a long period of time but also for successfully modifying and adapting source code to maintain the same tools, tactics, and infrastructure since at least 2005. Evidence shows that the group prioritises targets, most likely works in shifts in a collaborative environment, and builds malware from a coherent development plan. The group has had the capability to infect air-gapped networks since 2005. APT30 uses a suite of tools that includes downloaders, backdoors, a central controller, and several components designed to infect removable drives and cross-air-gapped networks to steal data. APT30 frequently registers its own DNS domains for malware CnC activities. While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches.
APT31 (G0128, Zirconium, Judgment_Panda, Bronze_Vinewood, Red_keres, Violet_Typhoon)	APT31 is a China-nexus cyber espionage actor, active since at least 2016, focused on obtaining information that can provide the Chinese government and state-owned enterprises with political, economic, and military advantages. Also has targeted individuals associated with the 2020 US presidential election and prominent leaders in the international affairs community.

Group Name	Description
APT40 (G0065, Leviathan, TEMP.Periscope, Periscope_Group, Mudcarp, Kryptonite_Panda, Gadolimium, Bronze_Mohawk, Gingham_Typhoon)	A Chinese cyber espionage group that has been attributed to the Ministry of State Security's (MSS) Hainan State Security Department, has been active since at least 2009. The group targets countries strategically important to "The Belt and Road Initiative", global organisations, and the following sectors: academia, aerospace/aviation, biomedical, defence industrial base, government, healthcare, manufacturing, and maritime. Also, they conducted campaigns against regional entities in areas such as Southeast Asia and targeted transportation across the US, Canada, Europe, the Middle East, and Southeast Asia. On July 19, 2021, the U.S. Department of Justice (DOJ) unsealed an indictment against four APT40 cyber actors for their illicit computer network exploitation activities via front company Hainan Xiandun Technology Development Company
APT41 (G0096, Wicked_Panda, Double_Dragon, TG-2633, Wicked_Spider, Bronze_Atlas, Red_Kelpie, Blackfly)	Prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control. Active since at least 2012, APT41 has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. APT41 conducted a campaign between May 2021 and February 2022 that successfully compromised at least six U.S. state government networks through the exploitation of vulnerable Internet-facing web applications. During this campaign, APT41 was quick to adapt and use publicly disclosed as well as zero-day vulnerabilities for initial access, and in at least two cases re-compromised victims following remediation efforts. The goals of C0017 are unknown, however, APT41 was observed exfiltrating Personal Identifiable Information. The group was named by the United States Department of Justice in September 2020 in relation to charges brought against five Chinese and two Malaysian nationals for allegedly compromising more than 100 companies around the world. Related to Ministry of State Security, PRC, started to be active in 2009, main targets are high-tech, gaming industry, finance, telecom, media, high-level education, travel industry and medical service in Europe, North America and Asia.
Admin@338 (G0018)	China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organisations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors.

Group Name	Description
Aoqin Dragon (G1007)	Suspected Chinese cyber espionage threat group that has been active since at least 2013. Aoqin Dragon has primarily targeted government, education, and telecommunication organisations in Australia, Cambodia, Hong Kong, Singapore, and Vietnam. This group uses one of three infection strategies: ■ using a document exploit and tricking the user into opening a weaponized Word document to install a backdoor; ■ luring users into double-clicking a fake Anti-Virus to execute malware in the victim's host; ■ forging a fake removable device to lure users into opening the wrong folder and installing the malware successfully on their system.
Aquatic Panda (G0143)	Suspected China-based threat group with a dual mission of intelligence collection and industrial espionage. Active since at least May 2020, Aquatic Panda has primarily targeted entities in the telecommunications, technology, and government sectors. In December of 2023, they made an attempt to use a modified version of the Log4j exploit to attack an unnamed "large academic institution". Is believed to operate under the Chinese Ministry of State Security (MSS), helping to enhance regional security, promote economic stability, and advance technological development efforts.
Axiom (G0001, Group_72)	Suspected a Chinese cyber espionage group that has targeted the aerospace, defence, government, manufacturing, and media sectors since at least 2008. Axiom has been responsible for directing highly sophisticated cyber espionage operations against numerous Fortune 500 companies, journalists, environmental groups, pro-democracy groups, software companies, academic institutions, and government agencies worldwide for at least six years (from 2008 to 2014).
BlackTech (G0098, Palmerworm, Circuit_ Panda, Huapi, Temp. Overboard)	Suspected Chinese cyber espionage group that has primarily targeted organisations in East Asia — particularly Taiwan, Japan, and Hong Kong — and the US since at least 2013. Related to the PLA, main targets are Japan, South Korea, the US and Taiwan. Target domains consist of government, military, high-tech and telecom
Chimera (G0114)	Suspected China-based threat group that has been active since at least 2018 targeting the semiconductor industry in Taiwan as well as data from the airline industry. From 2019 till 2021 the group has been abusing Microsoft and Google cloud services with the goal of exfiltrating data across a broad range of target organisations.

Group Name	Description
Earth Lusca (G1006)	A suspected China-based cyber espionage group that has been active since at least April 2019. Earth Lusca has targeted organisations in Australia, China, Hong Kong, Mongolia, Nepal, the Philippines, Taiwan, Thailand, Vietnam, the United Arab Emirates, Nigeria, Germany, France, and the United States. Targets included government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organisations, telecommunications companies, religious movements banned in China, and cryptocurrency trading platforms; security researchers assess some Earth Lusca operations may be financially motivated. In mid-2021 Earth Lusca group targeted organisations globally via a campaign that used traditional social engineering techniques such as spear-phishing and watering holes. The list of its victims includes high-value targets such as government and educational institutions, religious movements, pro-democracy and human rights organisations in Hong Kong, and COVID-19 research organisations.
HAFNIUM (G0125)	Likely a State-sponsored cyber espionage group operating out of China that has been active since at least January 2021. HAFNIUM primarily targets entities in the US across several industry sectors, including infectious disease researchers, law firms, higher education institutions, defence contractors, policy think tanks, and NGOs.
IndigoZebra (G0136)	A suspected Chinese cyber espionage group that has been targeting Central Asian governments since at least 2014. The latest known incident happened in mid-2021 when the Afghanistan National Security Council employees were attacked by xCaon backdoor within a spear-phishing email campaign.
Mofang (G0103, Superman)	Likely a China-based cyber espionage group, named for its frequent practice of imitating a victim's infrastructure. This adversary has been observed since at least May 2012 conducting focused attacks against the government and critical infrastructure in Myanmar, as well as several other countries and sectors including military, automobile, and weapons industries.
Mustang Panda (G0129, TA416, RedDelta, Bronze_President)	China-based cyber espionage threat actor was first observed in 2017 but may have been conducting operations since at least 2014. Mustang Panda has targeted government entities, nonprofits, religious, and other non-governmental organisations in the U.S., Europe, Mongolia, Myanmar, Pakistan, and Vietnam, among others.

Group Name	Description
Naikon (G0019, PLA Unit 78020, Lotus_Panda, Camera_Shy)	Assessed to be a state-sponsored cyber espionage group attributed to the Chinese People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020). Active since at least 2010, Naikon has primarily conducted operations against the government, military, and civil organisations in Southeast Asia, as well as against international bodies such as the United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN).
Rocke (G0106)	Alleged a Chinese-speaking adversary whose primary objective appeared to be cryptojacking or stealing victim system resources for the purposes of mining cryptocurrency.
TA459 (G0062)	Threat group is believed to operate out of China and has targeted countries including Russia, Belarus, Mongolia, and the USA. In April 2022 they targeted US-based media personnel with emails containing a malicious RoyalRoadRTF attachment. This group is probably related to APT31.
Tonto Team (G0131, Earth_Akhlut, Bronze_Huntley, CactusPete, Karma_Panda)	Suspected of a Chinese state-sponsored cyber espionage threat group that has primarily targeted South Korea, Japan, Taiwan, and the United States since at least 2009; by 2020 they expanded operations to include other Asian as well as Eastern European countries. Tonto Team has targeted government, military, energy, mining, financial, education, healthcare, and technology organisations, including through the Heartbeat Campaign (2009-2012) and Operation Bitter Biscuit (2017).
UNC3886	UNC3886 group associated with the novel VMware ESXi hypervisor malware framework disclosed last September. The UNC3886 cyber espionage group comes with unique capabilities in how they operate on-network as well as the tools they utilise in their campaigns, and have been observed targeting firewall and virtualization technologies that lack EDR support. Their ability to manipulate firewall firmware and exploit a zero-day indicates they have curated a deeper level of understanding of such technologies. UNC3886 has modified publicly available malware, targeting *nix operating systems.
Winnti Group (G0044)	Winnti Group is a threat group with Chinese origins that has been active since at least 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting. Some reports suggest a number of other groups, including Axiom, APT17, and Ke3chang, are closely linked to the Winnti Group.

Annex 2.

North Korea's most used TTP's from attack.mitre.org

Code	Name
T1071.001	Application Layer Protocol: Web Protocols
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1059.001	Command and Scripting Interpreter: PowerShell
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1059.005	Command and Scripting Interpreter: Visual Basic
T1543.003	Create or Modify System Process: Windows Service
T1485	Data Destruction
T1005	Data from Local System
T1561.002	Disk Wipe: Disk Structure Wipe
T1189	Drive-by Compromise
T1203	Exploitation for Client Execution
T1105	Ingress Tool Transfer
T1106	Native API
T1083	File and Directory Discovery
T1027	Obfuscated Files or Information
T1562.004	Impair Defences: Disable or Modify System Firewall
T1566.001	Phishing: Spearphishing Attachment
T1057	Process Discovery
T1053.005	Scheduled Task/Job: Scheduled Task
T1056.001	Input Capture: Keylogging

Annex 3.

Iran's most used TTP's from attack.mitre.org

Code	Name
T0852	Screen Capture
T0853	Scripting
T1003.001	OS Credential Dumping: LSASS Memory
T1003.004	OS Credential Dumping: LSA Secrets
T1003.005	OS Credential Dumping: Cached Domain Credentials
T1012	Query Registry
T1021.001	Remote Services: Remote Desktop Protocol
T1021.004	Remote Services: SSH
T1027	Obfuscated Files or Information
T1027.002	Software Packing
T1033	System Owner/User Discovery
T1046	Network Service Discovery
T1048.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol
T1053.005	Scheduled Task/Job: Scheduled Task
T1059.001	Command and Scripting Interpreter: PowerShell
T1059.005	Command and Scripting Interpreter: Visual Basic
T1070.004	Indicator Removal: File Deletion
T1071.001	Application Layer Protocol: Web Protocols
T1071.004	Application Layer Protocol: DNS
T1078	Valid Accounts
T1105	Ingress Tool Transfer
T1110	Brute Force
T1113	Screen Capture
T1140	Deobfuscate/Decode Files or Information
T1204.001	User Execution: Malicious Link
T1204.002	User Execution: Malicious File

Code	Name
T1505.003	Server Software Component: Web Shell
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1552.001	Unsecured Credentials: Credentials In Files
T1555	Credentials from Password Stores
T1555.003	Credentials from Web Browsers
T1560.001	Archive Collected Data: Archive via Utility
T1566.001	Phishing: Spearphishing Attachment
T1566.002	Phishing: Spearphishing Link
T1588.002	Obtain Capabilities: Tool

Annex 4.

Russia's most used TTP's from attack.mitre.org

Code	Name
T1003.001	OS Credential Dumping: LSASS Memory
T1003.002	OS Credential Dumping: Security Account Manager
T1003.003	OS Credential Dumping: NTDS
T1005	Data from Local System
T1007	System Service Discovery
T1012	Query Registry
T1016	System Network Configuration Discovery
T1016.001	System Network Configuration Discovery: Internet Connection Discovery
T1018	Remote System Discovery
T1021.001	Remote Services: Remote Desktop Protocol
T1021.002	Remote Services: SMB/Windows Admin Shares
T1021.006	Remote Services: Windows Remote Management
T1025	Data from Removable Media
T1027	Obfuscated Files or Information: Command Obfuscation
T1027.001	Binary Padding
T1027.002	Software Packing
T1027.005	Obfuscated Files or Information: Indicator Removal from Tools
T1027.010	Command Obfuscation
T1033	System Owner/User Discovery
T1036	Masquerading
T1036.004	Masquerading: Masquerade Task or Service
T1036.005	Masquerading: Match Legitimate Name or Location
T1039	Data from Network Shared Drive
T1040	Network Sniffing
T1041	Exfiltration Over C2 Channel
T1047	Windows Management Instrumentation

Code	Name
T1048.002	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
T1049	System Network Connections Discovery
T1053	Scheduled Task/Job: Scheduled Task
T1056.001	Input Capture: Keylogging
T1057	Process Discovery
T1059	Command and Scripting Interpreter: PowerShell
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1059.005	Command and Scripting Interpreter: Visual Basic
T1059.006	Command and Scripting Interpreter: Python
T1059.007	Command and Scripting Interpreter: JavaScript
T1068	Exploitation for Privilege Escalation
T1069	Permission Groups Discovery: Domain Groups
T1070.001	Indicator Removal: Clear Windows Event Logs
T1070.004	Indicator Removal: File Deletion
T1070.006	Indicator Removal: Timestomp
T1071.001	Application Layer Protocol: Web Protocols
T1071.003	Application Layer Protocol: Mail Protocols
T1074.001	Data Staged: Local Data Staging
T1074.002	Data Staged: Remote Data Staging
T1078	Valid Accounts
T1078.002	Domain Accounts
T1078.004	Cloud Accounts
T1082	System Information Discovery
T1083	File and Directory Discovery
T1087.002	Account Discovery: Domain Account
T1090	Proxy
T1090.003	Proxy: Multi-hop Proxy
T1098	Account Manipulation
T1098.002	Account Manipulation: Additional Email Delegate Permissions
T1102	Web Service

Code	Name
T1102.002	Web Service: Bidirectional Communication
T1105	Ingress Tool Transfer
T1106	Native API
T1110	Brute Force
T1112	Modify Registry
T1113	Screen Capture
T1114.002	Email Collection: Remote Email Collection
T1119	Automated Collection
T1120	Peripheral Device Discovery
T1133	External Remote Services
T1135	Network Share Discovery
T1140	Deobfuscate/Decode Files or Information
T1189	Drive-by Compromise
T1190	Exploit Public-Facing Application
T1195	Supply Chain Compromise: Compromise Software Supply Chain
T1199	Trusted Relationship
T1203	Exploitation for Client Execution
T1204.001	User Execution: Malicious Link
T1204.002	User Execution: Malicious File
T1210	Exploitation of Remote Services
T1213	Data from Information Repositories
T1218.005	System Binary Proxy Execution: Mshta
T1218.011	System Binary Proxy Execution: Rundll32
T1221	Template Injection
T1485	Data Destruction
T1486	Data Encrypted for Impact
T1489	Service Stop
T1505.003	Server Software Component: Web Shell
T1518.001	Software Discovery: Security Software Discovery
T1543.003	Create or Modify System Process: Windows Service

Code	Name
T1546.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1547.004	Boot or Logon Autostart Execution: Winlogon Helper DLL
T1550.001	Use Alternate Authentication Material: Application Access Token
T1553.002	Subvert Trust Controls: Code Signing
T1555.003	Credentials from Password Stores: Credentials from Web Browsers
T1558.003	Steal or Forge Kerberos Tickets: Kerberoasting
T1560	Archive Collected Data
T1560.001	Archive Collected Data: Archive via Utility
T1562.001	Impair Defences: Disable or Modify Tools
T1562.002	Impair Defences: Disable Windows Event Logging
T1562.004	Impair Defences: Disable or Modify System Firewall
T1564.003	Hide Artefacts: Hidden Window
T1566.001	Phishing: Spearphishing Attachment
T1566.002	Phishing for Information: Spearphishing Link
T1568	Dynamic Resolution
T1570	Lateral Tool Transfer
T1571	Non-Standard Port
T1583.001	Acquire Infrastructure: Domains
T1583.003	Acquire Infrastructure: Virtual Private Server
T1583.006	Acquire Infrastructure: Web Services
T1584.004	Compromise Infrastructure: Server
T1585.001	Establish Accounts: Social Media Accounts
T1586.002	Compromise Accounts: Email Accounts
T1587.001	Develop Capabilities: Malware
T1588.002	Obtain Capabilities: Tool
T1588.003	Obtain Capabilities: Code Signing Certificates
T1589.001	Gather Victim Identity Information: Credentials
T1591.002	Gather Victim Org Information: Business Relationships
T1595.002	Active Scanning: Vulnerability Scanning

Annex 5.

China's most used TTP's from attack.mitre.org

Code	Name
T1003.001	OS Credential Dumping: LSASS Memory
T1003.003	OS Credential Dumping: NTDS
T1005	Data from Local System
T1007	System Service Discovery
T1016	System Network Configuration Discovery
T1018	Remote System Discovery
T1021.001	Remote Services: Remote Desktop Protocol
T1021.002	Remote Services: SMB/Windows Admin Shares
T1027	Obfuscated Files or Information
T1027.010	Obfuscated Files or Information: Command Obfuscation
T1033	System Owner/User Discovery
T1036.005	Masquerading: Match Legitimate Name or Location
T1041	Exfiltration Over C2 Channel
T1047	Windows Management Instrumentation
T1049	System Network Connections Discovery
T1053.005	Scheduled Task/Job: Scheduled Task
T1056.001	Input Capture: Keylogging
T1057	Process Discovery
T1059.001	Command and Scripting Interpreter: PowerShell
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1069.001	Permission Groups Discovery: Local Groups
T1070.004	Indicator Removal: File Deletion
T1071.001	Application Layer Protocol: Web Protocols
T1074.001	Data Staged: Local Data Staging
T1078	Valid Accounts
T1082	System Information Discovery

Code	Name
T1083	File and Directory Discovery
T1087.001	Account Discovery: Local Account
T1087.002	Account Discovery: Domain Account
T1095	Non-Application Layer Protocol
T1098	Account Manipulation
T1105	Ingress Tool Transfer
T1114.002	Email Collection: Remote Email Collection
T1119	Automated Collection
T1133	External Remote Services
T1140	Deobfuscate/Decode Files or Information
T1190	Exploit Public-Facing Application
T1203	Exploitation for Client Execution
T1204.001	User Execution: Malicious Link
T1204.002	User Execution: Malicious File
T1213.002	Data from Information Repositories: Sharepoint
T1218.011	System Binary Proxy Execution: Rundll32
T1482	Domain Trust Discovery
T1543.003	Create or Modify System Process: Windows Service
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1560.001	Archive Collected Data: Archive via Utility
T1566.001	Phishing: Spearphishing Attachment
T1566.002	Phishing: Spearphishing Link
T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage
T1569.002	System Services: Service Execution
T1574.002	Hijack Execution Flow: DLL Side-Loading
T1583.001	Acquire Infrastructure: Domains
T1583.006	Acquire Infrastructure: Web Services
T1584.004	Compromise Infrastructure: Server
T1588.001	Obtain Capabilities: Malware
T1588.002	Obtain Capabilities: Tool
T1595.002	Active Scanning: Vulnerability Scanning



REGIONAL CYBER DEFENCE CENTRE