# The Chinese Government's Advanced Persistent Threats

Case Study

Jem Ramsey
Cybersecurity
University of West Florida
Pensacola, FL

## Abstract

With the increasing number of cyberattacks aimed towards companies and entire countries, Advanced Persistent Threats (APTs) are becoming a more prevalent force online.

With the goal of infiltration and gaining access into an organization, Advanced Persistent Threats are a sustained type of cyberwarfare where an attacker remains undetected in a system for a long period of time. The nation states notorious for having larger numbers of APTs are Russia, China, Iran, and United States. In this case study we will be focusing our attention on Chinese threats, specifically APT41.

## Introduction

In the recent years, China has been improving its hacking operations and become a more sophisticated force and mature adversary than it was in the past. The Chinese hacking force used to conduct operations that were more unsophisticated and sloppier in nature. Now their attacks are considered highly aggressive and are known for perpetrating attacks against companies and government around the world. They are considered one of the biggest digital threats to the United States.

In 2020 the Justice Department accused Chinese hackers of APT41 of affecting over 100 companies in the U.S and abroad as well. The goals behind APT groups fall into the categories of cyber espionage, financial gain, hacktivism, and destruction[2].

## Literature Review

Governmental and research agencies have found that recording and publishing these cyber threats is essential to mitigation of these future threats. Cyber operations that are well-organized usually follow a path or guideline. Example of popular ones are the MITRE ATT&CK framework or the Lockheed Martin Kill Chain. They are both used for identification and prevention of future cyber intrusions activity.

The Lockheed Martin Kill Chain includes seven steps that "enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, tactics and procedures."[8] In this case study we will be referring to an alternate operation lifecycle that also has seven phases- Target Identification, Reconnaissance, Gaining Access, Hiding Presence, Establishing Persistence, Execution, and Assessment.

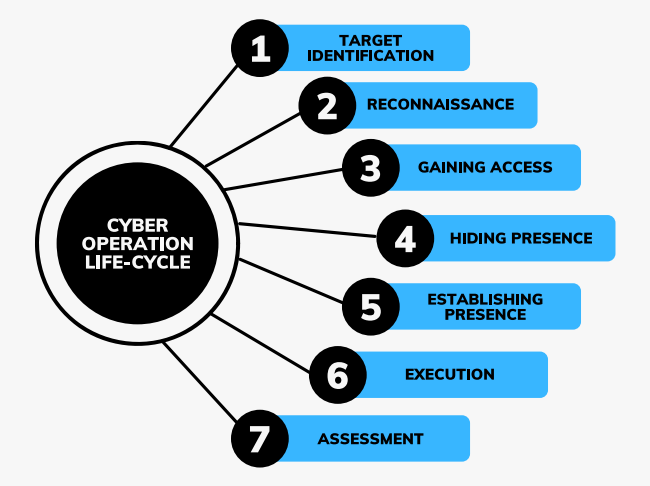


**Figure 1: Cyber Operation Lifecycle**

## Methodology

APT41 is a Chinese state-sponsored espionage threat group that is also financially motivated[1]. With proof of their existence dating back to 2012, they have been seen targeting technology, healthcare, telecom, video game, academic, and utilities industries in 14 countries. They have also been known to go by the name of 'Wicked Panda'.

According to CrowdStrike's observations, the majority of Chinese cyber threat activity has been seen from attackers working for China's Ministry of State Security (MSS)[2]. APT41

operational tempo is very high, which means there isn't a long period between each of their different attacks[5].

The question to be answered in this case study is: *Does APT41 conduct well-organized cyber operations to target governments and technology industries for political and financial gain?*

To answer this question, the Cyber Operations lifecycle referenced in the past section will be brought back to light. Each section will thoroughly be explained and will include specific methods and tactics.

1. **Target Identification**: The goal of this phase is to use passive reconnaissance to obtain information on the target without alerting them. The purpose of learning this information is to determine specific tactics that will be useful in moving forward with the rest of the operation[7]:
    a. Gather Victim Identity Information: This tactic is used to collect information on a selected target. There is a vast amount of information on the Internet that can be resourceful if found using the correct search engines or websites. Examples of sources can include LinkedIn for employee information, or social media accounts such as Instagram, Facebook, Twitter, etc.
    b. Gather Victim Network Information: This tactic is used by APTs to gain specific information about victim servers, IP address ranges, administrator identity information (such as names), and email addresses[6]. This information can be found from sites such as WhoIs and Wayback Machine. Wayback Machine shows past versions of a website and may show content that was up in the past, but then deleted due to being a security risk.
    c. Gather Victim Org Information: This tactic is used to gather specific information about the victim's organization by searching victim-owned websites or social media sites. This information may include the names of departments, business operation details, and roles/responsibilities of employers.
    d. Phishing for Information: Using this tactic is another way adversaries may be able to obtain sensitive information, such as login credentials or other useful personal information (ex. Date of Birth). It consists of tricking victims by using social engineering tactics, usually through email. Emails may include attachments or links posed as urgent that are used to gain information.
    e. Search Closed Sources: This tactic is used by adversaries to gain information from closed sources through means of purchasing. They can choose to purchase information from Threat Intel Vendors who may offer paid feeds with more data than is publicly available. They also have the option of purchasing information from sources such as the dark web or cybercrime black-markets.
    f. Search Open Technical Databases: This tactic can be used to obtain information found in online databases and repositories. DNS data may include information such as registered name servers and mail servers. Digital Certificates can also be found online that contain the name and location of the registered organization.
2. **Reconnaissance**: The goal of this next phase is to perform active reconnaissance to obtain information on the target, using direct interaction. This is the step in the process where an adversary makes real contact with the victim's system[7].
    a. Active Scanning: This tactic is used by APTs to scan victim's system using their network traffic. In order to scan IP address ranges, an adversary may use the Nmap tool. They may also perform vulnerability scanning against a system to determine a specific exploit to use in future phases.
    b. Gather Victim Host Information: This tactic can provide adversaries with information about a system such as the name, IP, and/or configuration details (ex. operating system and language). Means of obtaining this information is through use of Nmap and other similar tools.
3. **Gaining Access**: This phase consists of tactics that allow the adversary to gain initial access into the victim's network. The adversary is trying to put a "foot in the door" of the targeted system[9].
    a. Drive-by Compromise: This tactic allows adversaries to gain access of a system through a user browsing a website. Another method is by acquiring an Application Access Token.
    b. Exploit Public-Facing Application: Adversaries may exploit (take advantage of) a weakness in a system using software or commands to gain access. Common web vulnerabilities used by adversaries are listen in OWASP top 10 and CWE top 25.
    c. External Remote Services: Adversaries may take advantage of remote services using this tactic. An example of a remote service is a VPN which allows a user to connect to external locations/servers.

d. Phishing: This tactic is used when adversaries send phishing messages to gain access to the victim systems. This is considered a social engineering method and may be target specific or non-target specific. Adversaries use attachments, links, and third-party services to target victims.

e. Valid Accounts: This tactic is used when adversaries obtain credentials of victim accounts. It can assist APTs in not only gaining access to the user system, but to move to the next step in escalating privileges.

4. **Hiding Presence**: This phase is when adversaries compromise a victim system but still try to avoid detection. This is an essential phase to ensure the next phase "Establishing Presence" will not be short-lived[10]:

    a. Masquerading: This tactic may be used by APTs to manipulate features of a file, such as metadata, to appear legitimate or non-threatening. Adversaries may match legitimate name or location to increase defenses against being caught by the victim system.

    b. Modify Registry: This tactic is used when adversaries interact with the Windows Registry and hide configuration information to prepare for the next phase-Establishing Persistence.

    c. Obfuscated Files or Information: This tactic is used by adversaries when attempting to encrypt, encode, or obfuscate contents of a file to make difficult to analyze.

    d. Pre-OS Boot: A tactic used by adversaries to control the Pre-OS Boot mechanisms. They may modify components firmware or use bootkits. Bootkits are at a layer below the OS.

    e. Process Injection: This tactic is used when adversaries want to inject code into processes to assist in detection avoidance. This process includes execution of arbitrary code in the address space of a live process.

    f. Rootkits: The purpose of adversaries using this tactic is to hide any proof of malware by changing operating system calls. This method has been used in MacOS, Linux, and Windows systems.

    g. Signed Binary Proxy Execution: A tactic that may be used by APTs to prepare execution of malicious content by signing binaries with digital certificates that are seemingly trustworthy.

    h. Subvert Trust Controls: This tactic is used by adversaries to promote trust level of files so as not to raise suspicions by the users of the victim systems. This method is executed by stealing legitimate code signing materials to fake authenticity of a malicious program/file.

    i. Valid Accounts: A similar tactic mentioned in the previous phase, except in this phase the adversary uses the obtained credentials to login to a useful user account. They may use a mixture of other tactics as not to raise suspicions.

5. **Establishing Presence**: This phase is most successful when used in reference to the previous phase, Hiding Presence. Essentially, it is about an adversary maintaining or continuing access to the victim systems. This is done by creating multiple access points into a system so that if one access point gets closed, the adversary won't lose complete access[11]:

    a. BITS Jobs: This tactic is used when adversaries use Windows Background Intelligent Transfer Service (BITS) to download or execute after running malicious code. It may create long-standing jobs or clean up proof of any malicious jobs running in the first place.

    b. Boot or Logon Initialization Scripts: This tactic is used to execute certain boot or logon initialization scripts automatically.

    c. Create Account: This tactic may be used by adversaries to create accounts that are used to maintain valuable access to a system. They may create primary or secondary accounts as a backup if one has not been hidden well enough.

    d. Event Triggered Execution: When this tactic is used by an adversary, the system will run an event of choice when a predefined event occurs. There are two types of categories: Pre-event Triggers and Post-event Triggers.

    e. External Remote Services: This tactic is used with remote services such as VPNs. Adversaries may use the connections between these services (such as through an API) as another entryway into the system.

    f. Hijack Execution Flow: Adversaries may be seen using this tactic to execute malicious payloads of their own. Using methods such as DLL side-loading or path-interception can aid in establishing persistence in the victim systems

g. Pre-OS Boot: A tactic mentioned in the previous phase, Bootkits may also be used to assist adversaries in establishing and maintaining persistence in a system.

6. **Execution**: This phase consists of the adversary running malicious scripts on the victim system. This is where they carry out the attack by exploiting various vulnerabilities. How long this phase will last is dependent on how much time was spent on the Hiding Presence and Establishing Persistence phases.
    a. Command and Scripting Interpreter: A tactic used by adversaries to abuse command interpreters by executing commands or scripts maliciously. They may use remote services to achieve a remote command line execution.
    b. Exploitation for Client Execution: This tactic is used when adversaries use client applications to exploit vulnerabilities. These vulnerabilities can be found in various application categories such as Browser-based, Office and Third-Party Applications.
    c. Scheduled Task/Job: Adversaries use this tactic to schedule the execution of malicious code. There are various ways to perform task scheduling such as using the Windows Task Scheduler or the Cron utility.
    d. System Services: This tactic is used by adversaries when using system services or daemons to execute malicious commands. They may be used for temporary execution.
    e. Windows Management Instrumentation: This tactic is used by adversaries when using Windows Management Instrumentation to execute malicious commands or programs.
7. **Assessment**: In this phase the adversaries look over their operation with a bird's eye view. They might answer the question "Were the main goals achieved?'. If the answer is yes, then they would need to decide if it is worth it to continue with operation. The longer the operation continues, the higher chance they have of being detected by the victim systems.

## Results

### APT41 Techniques

These are the techniques that APT41 has been recorded using, gathered by MITRE ATT&CK:

1. **Target Identification**: While APT41's goal is not completely known there is evidence of the threat group exfiltrating personal identifiable information to choose their specific targets (use of Valid Accounts technique). The group focuses on high-profile victims and multiple government systems. Their three main goals have been described as theft of intellectual property, surveillance, and financial theft[15].
2. **Reconnaissance**: APT41 initially uses publicly available malware such as Meterpreter or Cobalt Strike to perform exploitation against victim systems. However, before deploying more advanced malware techniques they carry out the Reconnaissance phase to have a full understanding of how to have a better hold on the victim system. They may be using tools such as Nmap to scan their victims IP ranges for vulnerabilities.
3. **Gaining Access**:
    a. Exploit Public-Facing Application: APT41 exploited CVE -2020-10189 against Zoho ManageEngine Desktop Central, a desktop company. They also compromised Citrix Application Delivery Controllers (ADC) and gateway devices by using CVE-2019-19781[15].
    b. External Remote Services: APT41 used a VPN between a third-party app and a financial service to compromise an online payment service[16].
    c. Spearphishing Attachment: APT41 sent spearphishing emails with attachments to take advantage of victim systems[17]
    d. Compromise Software Supply Chain: APT41 injected malicious code into signed files and widely distributed them[18]
    e. Valid Accounts: APT41 used compromised login credentials to log on to various systems.
4. **Hiding Presence**:
    a. Code-Signing: APT41 used code-signing certificates to sign malware in targeting gaming and non-gaming industries[19].
    b. Indicator Removal on Host: APT41 removed evidence of its activity by clearing out Windows events, Bash histories, and file deleted from systems[27].
    c. Masquerade Task or Service: APT41 has created services to appear as trustworthy system tools[20].
    d. Match Legitimate Name or Location: APT41 advertises as a popular anti-virus software[20].
    e. Modify Registry: APT41 used malware called GOODLUCK to modify registry. The goal was to steal Indian airline credentials

f. Obfuscating Files or Information: APT41 used VMProtected binaries in various intrusions[22].
g. Bootkits: APT41 used Master Boot Record bootkits on Windows systems to hide their malicious files[23].

5. Establishing Presence:
   a. BITS Jobs: APT41 used BITSAdmin to install payloads[24].
   b. Registry Run Keys / Startup Folder: APT41 added a registry key to maintain presence for Cobalt Strike[25].
   c. Accessibility Features: APT41 used sticky keys in event triggered execution to maintain persistence onto their victim systems[26].
   d. Create of Modify Windows Service: APT41 modified Windows services to install backdoors. They created the StorSyncSvc service for the Cobalt Strike attack[27].
   e. Hijack Execution Flow: APT41 has used DLL Search Order Hijacking, DLL side-loading of their malware, and Dynamic Linker Hijacking[29].
   f. Bootkits: APT41 also used bootkits to maintain presence on a system[23].
   g. Scheduled Task: APT41 used an account they compromising to schedule a system task[29].
6. Execution:
   a. Command and Scripting Interpreter: APT41 used PowerShell, Windows Command Shell, and Unix shell (CVE-2019-19781) to execute malware[30].
   b. Exploitation for Client Execution: APT41 used these exploits when carrying out their attacks against governments and technological corporations: CVE-2012-0158, CVE-2015-1641, CVE-2017-0199, CVE-2017-11882, and CVE-2019-3396.
   c. Scheduled Task: APT41 scheduled system tasks to execute using compromised accounts[29].
   d. System Service Execution: APT41 used svchost.exe to execute system service for the Cobalt Strike operation[32].

## Conclusion

APT41's goals align with China's political and economic goals, such as to increase knowledge and development of the computing industry products and form surveillance operation against other countries.

Their targets include governments and gaming industries, but the targeting doesn't come to a halt there. They have been known to target Healthcare, Education, Telecommunications, Media, and Automotive industries. They have targeted various countries including but not limited to- France, Italy, Japan, Singapore, South Korea, Thailand, and the United States.

To answer the research question: *Does APT41 conduct well-organized cyber operations to target governments and technology industries for political and financial gain?*

APT41 conducts espionage operations using highly sophisticated and innovative methods/tools. APT41 uses a well-organized cyber operation beginning with identifying their target, gathering valuable information about that target, and then proceeding with gaining access into their victim systems. Next, they try to remain undetected and create a foothold on their target system by establishing presence on the system. Finally, they execute the main goal which is attacking the system. Their main targets are governments and technological industries to meet the goal of political and financial gain.

## REFERENCES


[1] *APT41, Group G0096 | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/groups/G0096/

[2] Advanced Persistent Threats (APTs) | Definition & Examples. (n.d.). Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

[3] *China hacked at least six U.S. state governments, report says*. (n.d.). NBC News. https://www.nbcnews.com/tech/security/china-hacked-least-six-us-state-governments-report-says-rcna19255

[4] Perlroth, N. (2021, July 19). How China Transformed Into a Prime Cyber Threat to the U.S. *The New York Times*. https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html

[5] *Advanced Persistent Threats (APTs) | Definition & Examples*. (n.d.). Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

[6] *Passive Reconnaissance - an overview | ScienceDirect Topics*. (2013). Sciencedirect.com. https://www.sciencedirect.com/topics/computer-science/passive-reconnaissance

[7] *Reconnaissance, Tactic TA0043 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/tactics/TA0043/

[8] Lockheed Martin. (2019). *Cyber Kill Chain*. Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[9] *Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/tactics/TA0001/

[10] *Defense Evasion, Tactic TA0005 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/tactics/TA0005/

[11] *Persistence - Enterprise | MITRE ATT&CK™*. (2015). Mitre.org. https://attack.mitre.org/tactics/TA0003/

[12] *Integrity Lifecycle Manager Help*. (n.d.). Support.ptc.com. Retrieved April 25,2022,from https://support.ptc.com/help/integrity_hc/integrity111_hc/en/index.html#page/IntegrityHelp/serv_trig_what_is_an_event_trigger.mif-1.html

[13] *Execution, Tactic TA0002 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/tactics/TA0002/

[14] *Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments | Mandiant*. (n.d.). Www.mandiant.com. https://www.mandiant.com/resources/apt41-us-state-governments

[15] *Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK™*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1190/

[16] *External Remote Services, Technique T1133 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1133/

[17] *Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1566/

[18] *Supply Chain Compromise, Technique T1195 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1195/

[19] *Subvert Trust Controls, Technique T1553 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1553/

[20] *Masquerading, Technique T1036 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1036/

[21] *[Report] Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation*. (n.d.). FireEye. https://content.fireeye.com/apt-41/rpt-apt41

[22] *Obfuscated Files or Information, Technique T1027 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1027/

[23] *Pre-OS Boot, Technique T1542 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. Retrieved April 26, 2022, from https://attack.mitre.org/techniques/T1542/

[24] *BITS Jobs, Technique T1197 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. Retrieved April 26, 2022, from https://attack.mitre.org/techniques/T1197/

[25] *Boot or Logon Autostart Execution, Technique T1547 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1547/

[26] *Event Triggered Execution, Technique T1546 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1546/

[27] *Create or Modify System Process, Technique T1543 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. Retrieved April 26, 2022, from https://attack.mitre.org/techniques/T1543/

[28] *Hijack Execution Flow, Technique T1574 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1574/

[29] *Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1053/

[30] *Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/techniques/T1059/

[31] *Exploitation for Client Execution, Technique T1203 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. Retrieved April 26, 2022, from https://attack.mitre.org/techniques/T1203

[32] *System Services, Technique T1569 - Enterprise | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. Retrieved April 26, 2022, from https://attack.mitre.org/techniques/T1569