THREAT INTELLIGENCE REPORT

The China Threat, In Brief

By Adam Hlavek

Introduction

Over the past two decades, the People's Republic of China has capitalized on the global connectivity of the internet age in ways no other nation has. Once regarded as a "second-tier" cyber power, China has aggressively and consistently built its national cyber program to the point where it is now considered one of the world's preeminent cyber players. A recent study ranked China as a "Most Comprehensive Cyber Power," second only to the United States. The ruling Chinese Communist Party (CCP) used a multi-pronged strategy to achieve this remarkable ascent, prioritizing computer science and technology education within China and creating a pipeline of talent for cyber military operations.

As the Chinese military and intelligence apparatus became more cyber-capable, units within the People's Liberation Army and contractors operating on behalf of the Ministry of State Security embarked on a systematic cyber espionage campaign. China obtained sensitive information held by foreign governments and stole intellectual property for cutting-edge technologies across numerous sectors by leveraging cyber alongside traditional intelligence collection methods and various forms of economic espionage. The campaign has, by any measure, been immensely successful.

China has directly utilized the information it has obtained via cyber espionage to improve its military capabilities. It has also used ill-gotten trade secrets to help its commercial companies compete on the global stage. Chinese corporations have been particularly successful at generating business in the developing world, building partnerships and promoting Chinese brands throughout Africa and the Middle East. Telecommunications giants Huawei and ZTE, for example, have already gained significant market share in Africa, partially due to multi-faceted support from the Chinese government. However, the prospect of having Chinese hardware built into telecommunications systems, particularly the emerging 5G cellular networks, has raised significant concerns over potential cyber espionage within the U.S. government. These concerns prompted the United States to ban the use of 5G technology from Chinese manufacturers within its borders and they have encouraged allies to do the same.

Following years of seeking parity with the Western world, China's leaders now seek to surpass their global and regional rivals and truly establish the China as the preeminent global superpower. China's near-term national strategy, the 14th Five Year Plan, released in October 2020, aims to reduce the country's reliance on foreign technology and build out domestic high-tech production capabilities. As evidenced by the numerous examples that follow here, cyber espionage will no doubt remain a centerpiece of the Chinese strategy to achieve these goals.

China’s Strategic Goals

1. Cement Status as a Great Power

In the early days of Commust rule, China lacked the military might or economic prosperity of superpowers like the United States or regional rivals like Japan. Following decades of power struggles and major societal upheavals resulting from World War II, the split with Nationalist Taiwan, and the subsequent Cultural Revolution, the party’s leaders became determined to remake China into a modern and prosperous nation, seeking to reassert China as a global center of influence and prestige.

After having fully transitioned to a quasi-capitalist, industrialized superpower, current Chinese President Xi Jinping has sought to accelerate this transformation. Under Xi, China has simultaneously increased its participation in international organizations and sought to broadly export its goods, services, and values abroad. The most notable examples of this are the Belt and Road Initiative, which seeks to create a vast land and sea infrastructure network connecting numerous cities and nations across East Asia and Europe, and the Made in China 2025 campaign, which aims to make China the preeminent global producer and seller of high-technology goods. In 2017, China also unveiled its National Artificial Intelligence Plan, which seeks to make it the “world’s major AI innovation center” by 2030.

Historical Cyber Examples:

- Internet Governance Initiatives
- Technology Investment and Partnerships in the Developing World

Recent Cyber Examples:

- 2020: Technology Investment Initiative

2. Preserve Communist Party Control and Quell Dissent

Despite the quasi-capitalist structure of modern China, the Chinese Communist Party represents the unquestioned center of power within Chinese society. In a distinct contrast with Western democracies, the CCP views domestic stability and the spread of anti-government sentiment as national security issues no different from foreign threats. Throughout his time as President and General Secretary, Xi Jinping has sought to consolidate his power and systematically increase control over dissenters, minority groups, and independence movements within mainland China and their supporters abroad.

To accomplish this, the Chinese state has institutionalized censorship and surveillance, investing heavily in technologies designed to limit free speech across China’s portion of the internet and establishing a variety of electronic surveillance programs. These tools are most frequently trained upon China’s most marginalized populations, including the Muslim Uyghirs of Xinjiang Province and the Tibetan independence movement, as well as domestic critics of the regime and high profile foreign visitors of interest to Chinese security services.

To ensure their control of the flow of information and to make the nation's infrastructure more defensible, China's leadership chose to connect the country to the internet in a manner unlike nearly any other nation. With key exchange and peering points required to physically reside within Chinese territory, the government has the ability to quickly isolate its networks from the outside world should it choose to do so.

Historical Cyber Examples:

- Institutionalized Censorship of the Internet
- Electronic Surveillance of Religious Institutions

Recent Cyber Examples:

- RedDelta
- Great Firewall "Enhancements"
- Android Surveillanceware Campaigns

3. Establish Military, Political, and Economic Preeminence within APAC Region

Second only to the CCP's desire to maintain internal stability within mainland China is the People's Republic of China's determination to cement itself as the dominant power within the Asia Pacific region. Japan, South Korea, and Taiwan have long represented economic and political competitors, but emerging markets in developing Southeast Asian nations also challenge China's economic dominance. The presence of U.S. military forces in Japan and South Korea, China's decades-long stand-off with Taiwan, and tensions surrounding the ever unpredictable North Korean regime also present military challenges to China's primacy throughout the region.

China's desire to exert control over the South China Sea represents one of the more concerning flashpoints brought about by this longstanding goal to become a dominant world power. The South China Sea boasts significant fossil fuel deposits and represents a critical trade route for many countries in the region. As such, multiple nations have laid claims of territorial sovereignty over portions of its waters. In an aggressive bid to undermine such claims, China has undertaken a massive effort to build multiple military outposts in the Spratly and Paracel Islands and has gone so far as to create new and artificial islands to bolster its own position and send a message to those who would challenge them.

As is often the case, the China has leveraged cyber operations to collect information on its competitors in the region. This has extended to governments, businesses, and civil society, as evidenced by several of the threat campaigns described in more detail on the following page.

Historical Cyber Examples:

- 2018: BRONZE PRESIDENT Targeting of NGOs and Political Organizations

Recent Cyber Examples:

- 2018-2020: Targeting of Southeast Asian Governments
- 2019 - 2020: Influence Operations Targeting Hong Kong and Taiwan
- Operations Targeting Taiwanese Government
- Operation Chimera / Operation Skeleton Key
- Targeting of Malaysian Government Officials

4. Achieve Military and Technological Parity with Western Rivals

China has long sought to establish military parity with the United States and its long time allies Australia and New Zealand. Following World War II and the Korean War, the U.S. had established a significant military presence across the Pacific. CCP leadership was keenly aware that China lacked the technological and economic might of the world's superpowers despite China's vast territory, burgeoning population, and natural resources.

At the dawn of the internet age, CCP leadership saw an opportunity to level the playing field and embarked on an unprecedented, decades-long campaign to obtain that parity through the deliberate theft of intellectual property across a myriad of technologies. Cyber espionage became the centerpiece of those efforts, which proved to be devastatingly effective. There are multiple examples, going back over a decade, of Chinese theft of U.S. and other foreign military technology via cyber espionage, including missile systems, aircraft, and naval vessels, among others. To further facilitate these goals, Chinese intelligence entities have also sought to aggressively obtain information on members of Western governments, militaries, and contractors, and have collected huge swaths of data on American citizens following successful penetrations of organizations like the U.S. Office of Personnel Management (OPM) and the Equifax credit bureau.

Such operations have not been confined to military technologies or government entities. The recent pandemic provides yet another example of Chinese attempts to illicitly obtain intellectual property. In May of 2020, a joint announcement from the FBI and CISA indicated that China-sponsored actors had compromised U.S. organizations conducting COVID-19 research.

Historical Cyber Examples:

- 2003-2007: Titan Rain Intrusions
- Advanced Weapons System Breaches
- 2014: OPM Breach

Recent Cyber Examples:

- 2018: Compromise of U.S. Navy Contractor
- 2020: Targeting of COVID-19 Research Organizations
- 2020: MSS Hackers Targeting Intellectual Property

Recent Chinese Threat Campaigns

To summarize the threat at a more tactical level, the following sections highlight several of the most recent and notable Chinese state-sponsored campaigns uncovered by cybersecurity researchers. Each section identifies a sample of the countries and sectors targeted by a given group, and the behaviors or tactics, techniques, and procedures (TTPs) utilized to succeed in their objectives. Footnotes provide links to further, more detailed, reading.

BlackTech

Overview

BlackTech is a threat group known primarily for conducting cyber espionage operations against targets in East Asia, with a focus on Taiwan and Japan. The group has likely been active for a number of years and is responsible for several separate campaigns leveraging overlapping infrastructure. BlackTech often abuses legitimate software tools and processes to achieve its goals, using stolen digital certificates and API hooking among other techniques.

Recent Activity

Recent reporting confirms that BlackTech remains active and has continued to develop new custom malware. Researchers at Symantec, who track this group as Palmerworm, noted BlackTech activity throughout 2019 and 2020 with the group leveraging new strains of malware to target multiple sectors in Taiwan, Japan, and China.

To date, no private sector cybersecurity companies have publicly attributed activity to BlackTech. However, in August of 2020, the Taiwanese government asserted that the group was working on behalf of the Chinese Communist Party and had been involved in cyber operations targeting multiple Taiwanese government and commercial entities.

Known Targets	Technology, engineering, finance, and government sectors in Taiwan, Japan, Hong Kong, and the U.S., with a focus on East Asia.

Sample TTPs	Various custom backdoors, including the well-documented PLEAD (also tracked as TSCookie).
	Deployment of PLEAD using compromised legitimate software, potentially via compromised routers and man-in-the-middle attacks.
	Use of legitimate system tools (Putty, PSExec, etc.) for malicious purposes (i.e., “living-off-the-land” tactics).
	Use of the DLL-hijacking Waterbear modular malware.
Also Known As	Palmerworm, CIRCUIT PANDA

APT41/Winnti

Overview

APT41 represents one of the most prolific Chinese state-sponsored threats. Incarnations of APT41 began to appear in the early 2010s, and the group is believed to have been behind intrusions into a wide variety of sectors, including the healthcare, pharmaceutical, telecommunications, and video game industries, with victims on nearly every continent. Over the years, the group has leveraged a variety of custom malware, including a Trojan that came to be known as Winnti.

The group is probably best known for a series of software supply chain attacks where the threat actors obtain access to software provider systems and inject malicious code into the victim’s legitimate software, often managing to distribute the poisoned software through the victim’s established channels. Such attacks are especially challenging to detect and mitigate from a consumer perspective, as end users and system administrators invariably trust software that has been downloaded directly from the publisher. Notably, some of the individuals comprising APT41 appear to have engaged in not just state-sponsored espionage, but have also dabbled in operations designed to reap personal financial gain.

There is notable overlap and a significant lack of clarity within the commercial cybersecurity community on precisely which groups are behind the many intrusions that have been lumped together under the Winnti umbrella. Some notable software supply chain attacks that have been potentially linked to the group by various cybersecurity researchers include the CCleaner, NetSarang, and Asus Live Update compromises. Given the history of software tool sharing amongst Chinese threat actors and the likelihood that multiple state-sponsored actors are targeting similar sets of victims, it becomes quite difficult to parse exactly which group may be behind a given intrusion, especially given the limited visibility that any one victim or vendor may have. In any case, the overarching tactics and targets described above can safely be ascribed to Chinese cyber operators, regardless of how specifically each discrete intrusion can be attributed.

Recent Activity

Another large-scale APT41 campaign occurred in early 2020, once again affecting a wide variety of industries in multiple global regions. The operators appeared to be systemically leveraging a number of recently identified high severity vulnerabilities, specifically in Cisco routers, Citrix infrastructure devices, and Zoho ManageEngine Desktop Central, an endpoint management software tool. Notably, the Citrix and Zoho vulnerabilities were also highlighted in a recent NSA advisory detailing public technical vulnerabilities known to have been actively exploited by Chinese state-sponsored actors.

The U.S. Department of Justice (DOJ) also shone a light on APT41 in September of 2020, unsealing three indictments that brought charges against five Chinese nationals and two Malyasians for a sweeping series of network intrusions. The DOJ linked the activity to a Chinese company known as Chengdu 404 Network Technology, which likely operates at the behest of the Chinese Ministry of State Security. The indictments stated that the hackers were responsible for intrusions across over 100 victim organizations in numerous countries. One of the indictments charged the two Malyasian individuals with profiting from information stolen from video game companies that was provided to them by Chinese actors. Both men were apprehended by Malaysian authorities. The operators apparently also participated in ransomware and crypto-jacking attacks, which highlight the type of for-profit criminal endeavors the group has undertaken apart from their more traditional information gathering operations.

Known Targets	Numerous sectors, including healthcare, media, and video games Multiple countries including the U.S., Japan, South Korea, India, Australia, and the U.K.
Sample TTPs	Software supply chain attacks which modified legitimate software to facilitate intrusions against the software's customers.
	Use of stolen digital certificates to sign malware.
	Command and control (C2) dead drops leveraging seemingly legitimate web pages to surreptitiously pass encoded instructions to deployed malware.
	Exploitation of remote access or internet facing services to gain initial access to victim networks.
Also Known As	Barium, Winnti, Wicked Panda, Wicked Spider

APT40

Overview

Likely active since at least 2013, APT40 is a Chinese threat group with a predominant focus on nations and issues related to the South China Sea, a region China has claimed territorial sovereignty over despite numerous disputes. The group has repeatedly targeted shipbuilding, maritime, and engineering entities, as well as government and academic institutions within multiple countries bordering the South China Sea. The group has leveraged a variety of malicious software, including publicly available tools such as Cobalt Strike and custom tools, some of which overlap with other known Chinese groups. Analysis of data obtained from APT40 infrastructure showed malware administrators accessing the group's servers from Hainan, China, which strongly suggests Chinese state sponsorship when coupled with the group's targeting patterns.

Recent Activity

Recent analysis released by Microsoft indicates that APT40 threat actors have on multiple occasions attempted to use cloud-native services within Azure to conduct malicious C2. Although the activity was identified and disrupted, the threat actors appear to have specifically designed malware to abuse proprietary cloud services including the Outlook Task API, OneDrive API, and Microsoft Graph API.

APT40 was also among the Chinese groups Taiwan publicly accused of targeting multiple Taiwanese government agencies, alongside BlackTech, Mustang Panda, and other groups. This coincides with particularly aggressive Chinese cyber targeting of Taiwan's technology sector witnessed over the past couple years. Early 2020 also saw the Malaysian Computer Emergency Response Team (CERT) issue an advisory linking APT40 to an espionage campaign targeting Malaysian government officials.

Known Targets	U.S., Western Europe, Cambodia, Malaysia, and Taiwan with a focus on engineering, healthcare, government, maritime, and academic sectors.
Sample TTPs	Highly targeted spearphishing
	Frequent use of web shells (such as China Chopper) and common web protocols for C2
	Use of legitimate remote services such as SSH and RDP to conduct reconnaissance and move laterally within victim networks
	Attempts to abuse proprietary Microsoft Azure cloud services
Also Known As	GADOLINIUM, Leviathan, TEMP.Periscope

Mustang Panda

Overview

Mustang Panda is a Chinese state-sponsored threat group with a history of targeting various NGOs (non-governmental organizations), minority groups, and political entities within the Southeast Asian region. The group has also been noted targeting Western think tanks and NGOs with a nexus to Chinese minority groups. The group has likely been active since at least 2017.

Mustang Panda frequently relies on phishing lures centered around themes directly relevant to their targeted victims. These lures use official-looking documents written in the target's native language and containing information that would prompt the victim to open the attached document. These decoy documents frequently contain a .zip archive that executes a malicious loader when opened. This leads to the installation of the venerable PlugX malware or a Cobalt Strike Beacon.

Recent Activity

In the summer of 2020, Recorded Future reported newly identified activity related to Mustang Panda, which they track as RedDelta. Notably, the group targeted a number of organizations related to the Catholic Church. The researchers surmised that this activity was likely connected to the renewal of an agreement between the Vatican and the CCP and was likely designed to provide insights into the upcoming negotiations (a tactic often used by the Chinese government in political or business contexts).

Despite the campaign being identified in this way, it appears the threat actors resumed activity within days of the RedDelta report's publication. Additional research shows the group has remained active into Fall 2020 and has updated the malware loader they use to install their favored PlugX Remote Access Trojan (RAT).

Known Targets	Government entities, NGOs, and religious organizations in Mongolia, Hong Kong, Vietnam, Burma, India, and Pakistan; NGOs and think tanks abroad with a nexus to Southeast Asia and Chinese minority groups.
Sample TTPs	Use of multiple versions of the PlugX and Poison Ivy malware shared amongst Chinese threat actors.
	Infection chains delivering .zip files containing Windows Shortcut (.lnk) files, which in turn execute malicious code leading to the installation of PlugX or Cobalt Strike.
	The use of DLL side-loading tactics to install malicious software.
Also Known As	RedDelta, TA416, BRONZE PRESIDENT

TA410

Overview

In July 2019, several U.S. utility companies were targeted with a well-designed spearphishing campaign that impersonated a legitimate engineering licensing board to deliver the LookBack malware. This campaign was attributed to a group tracked as TA410, who proceeded to conduct a follow-on campaign once again targeting U.S. electric utilities in August of that year. Later media reports indicated that several smaller, regional public power utilities were among those targeted and that some were apparently unaware they had been targeted at all until they were informed by the FBI.

Recent Activity

Additional analysis later linked the LookBack phishing campaigns to another malware family dubbed FlowCloud. These two campaigns share a number of tactics, including the timeframes they were active, the use of malicious attachments contained in phishing emails, the installation techniques used, and overlapping infrastructure. Like LookBack, the FlowCloud campaign appears to have targeted victims in the utilities sector using well-crafted phishing emails impersonating professional organizations within the industry such as the American Society of Civil Engineers.

Notably, the researchers investigating TA410 identified similarities to the tactics used by TA429 (also known as APT10, listed on the following page). However, it is not fully clear whether the two groups' activity is truly related or whether this may have been a deliberate attempt by those responsible to plant "false flags" to help hide those behind the campaigns. The attempt to hide the campaign actors makes sense especially given the widespread media attention focused on APT10 due to the publication of multiple reports on the group and a related U.S. indictment of Chinese actors.

Known Targets	U.S. electric utilities
Sample TTPs	Sophisticated spearphishing
	Use of Microsoft Office documents with embedded malicious VBA macros
	Reconnaissance scanning against targets (specifically SMB)
Also Known As	None known

APT10

Overview

APT10 is a prolific and long-standing Chinese state-sponsored threat actor that has been active since at least 2006. The group's focus appears to be access enablement, providing inroads to support commercial and economic espionage against regional and international competitors including Japan, the United Kingdom, and the United States. Like so many threat groups, APT10 has historically used spearphishing tactics to gain initial footholds on victim networks. The operators then rely upon a combination of custom and publicly available hacking tools to move laterally throughout victim networks and establish persistence.

In 2017, details surrounding an APT10 campaign known as Operation Cloud Hopper came to light. The campaign focused on compromising IT managed service providers (MSPs), which are businesses that remotely manage IT infrastructure on behalf of their clients. Compromising these MSPs provided APT10 actors with access to the service providers as well as their customers. The MSPs' connections to their customer environments were at times used by APT10 to exfiltrate data from within customer environments. 2018 indictments by the U.S. Department of Justice revealed that those behind these campaigns worked for a company operating at the behest of the Ministry of State Security's Tianjin State Security Bureau. Later media reporting revealed just how widespread and successful this strategy had been, as several major MSPs appear to have been victimized by the group over the span of several years.

Additional reporting in 2019 asserted that APT10 actors had penetrated at least ten telecommunications or cellular provider companies across the globe in a campaign dubbed Operation Soft Cell. During this campaign, APT10 operators appeared to have been targeting Call Detail Records, which contain metadata regarding individual mobile subscribers including information such as device identifiers, locations, and call history. Such information would be considered highly useful to a foreign intelligence service and fits with APT10's history of facilitating access to sensitive datasets.

Recent Activity

Recently published research details continued cyber espionage activity being conducted by APT10 operators. This latest research provides evidence of yet another large-scale intrusion campaign targeting multiple global regions and sectors between Fall 2019 and Fall 2020. Most of the victims appear to have a connection to Japanese companies, with the automotive, pharmaceutical, and engineering sectors among those targeted. The campaign once again went after MSPs, the group's most favored target. During the campaign, APT10 was observed using a variety of dual-use and custom malware, extensively using DLL side-loading techniques to execute their malware and exploiting the recently publicized ZeroLogon vulnerability affecting Microsoft Windows systems.

Known Targets	Telecommunications, defense, construction, engineering, aerospace, and government sectors (among others) in the U.S., Europe, and Japan with a consistent focus on MSPs.
Sample TTPs	Spearphishing using malicious attachments
	DLL side-loading techniques
	Use of publicly available, quasi-legitimate remote access tool Quasar
	Use of various shared Chinese malware families, including Poison Ivy and PlugX
	Persistent targeting of MSPs for use as conduits to their customer networks
Also Known As	TA429, Menupass, Red Apollo, Stone Panda, Cicada

In Summary

As evidenced by the numerous examples of Chinese cyber campaigns waged against commercial, government, and nongovernmental entities around the world, it is clear that China has made cyber espionage a hallmark of its global strategy. Chinese leadership has focused massive resources on building out their nation's cyber capabilities to both secure the Communist Party's preeminence within the country and project power beyond its borders. Organizations working in an immensely broad number of fields have been targeted, ranging from renewable energy to nanotechnology to human rights. These broad and persistent targeting patterns are likely to continue the years to come.

Chinese tactics, techniques, and procedures have grown in sophistication as well. Once well known for executing "smash and grab" operations seeking to simply steal large amounts of data from their victims as quickly as possible, Chinese threat groups have since evolved. As the case studies above highlight, Chinese threat actors now seek new and novel ways to execute their attacks and hide them from network defenders. Innovation and collaboration have thus become paramount for defenders to identify and prevent such threats.

IronNet's mission is to provide companies, sectors, and nations with the cutting-edge tools required to defend against sophisticated threats in cyberspace. The behavioral analytics and threat intelligence built into our IronDefense platform provide the unique insights required to detect advanced threat actors, while our IronDome Collective Defense solution allows organizations to collectively defend against such threats using machine-speed correlation of data. We believe that technological innovation and collaboration amongst those seeking to secure cyberspace can ultimately overcome those seeking to divide and exploit it.