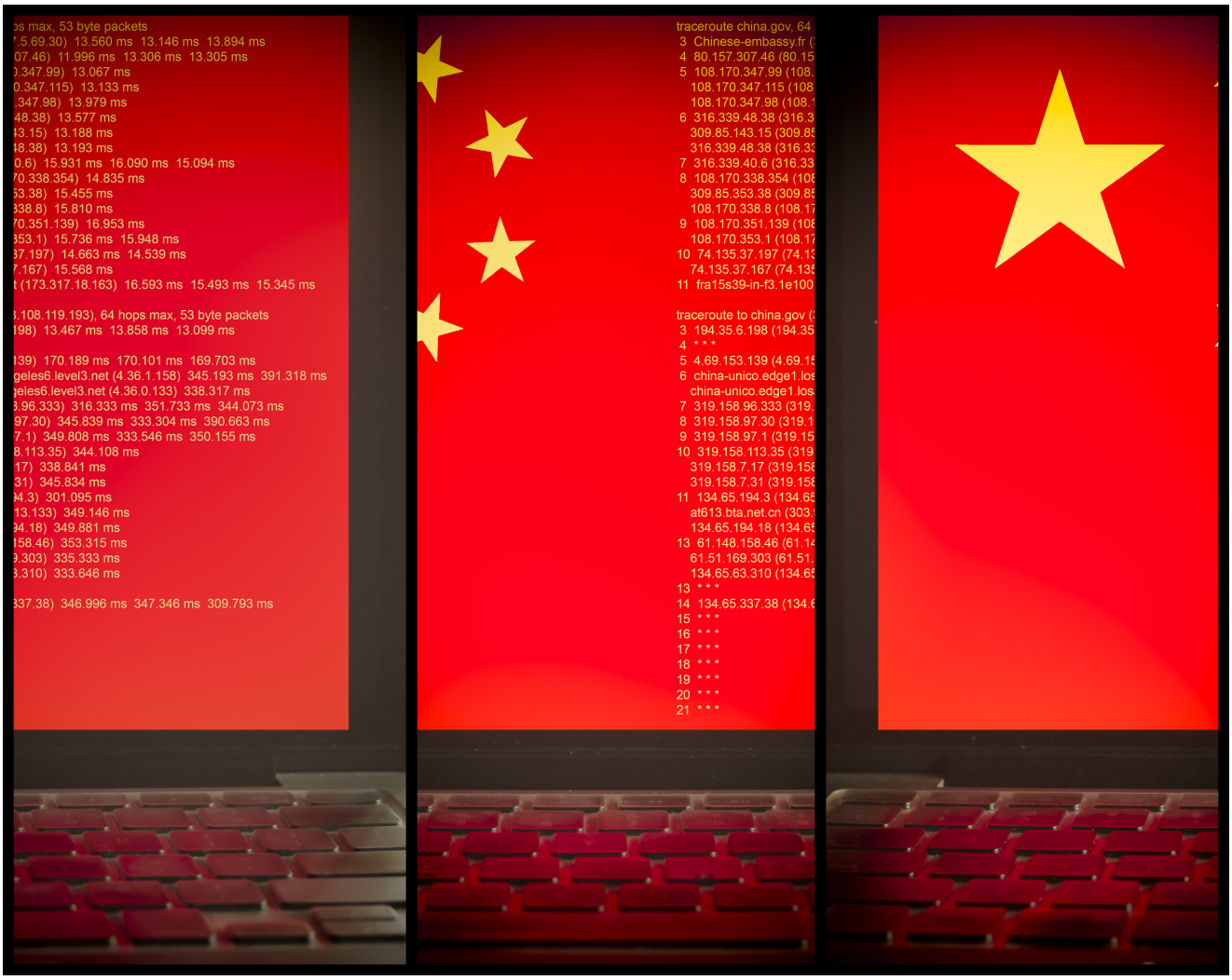
China cyber attacks: the current threat landscape

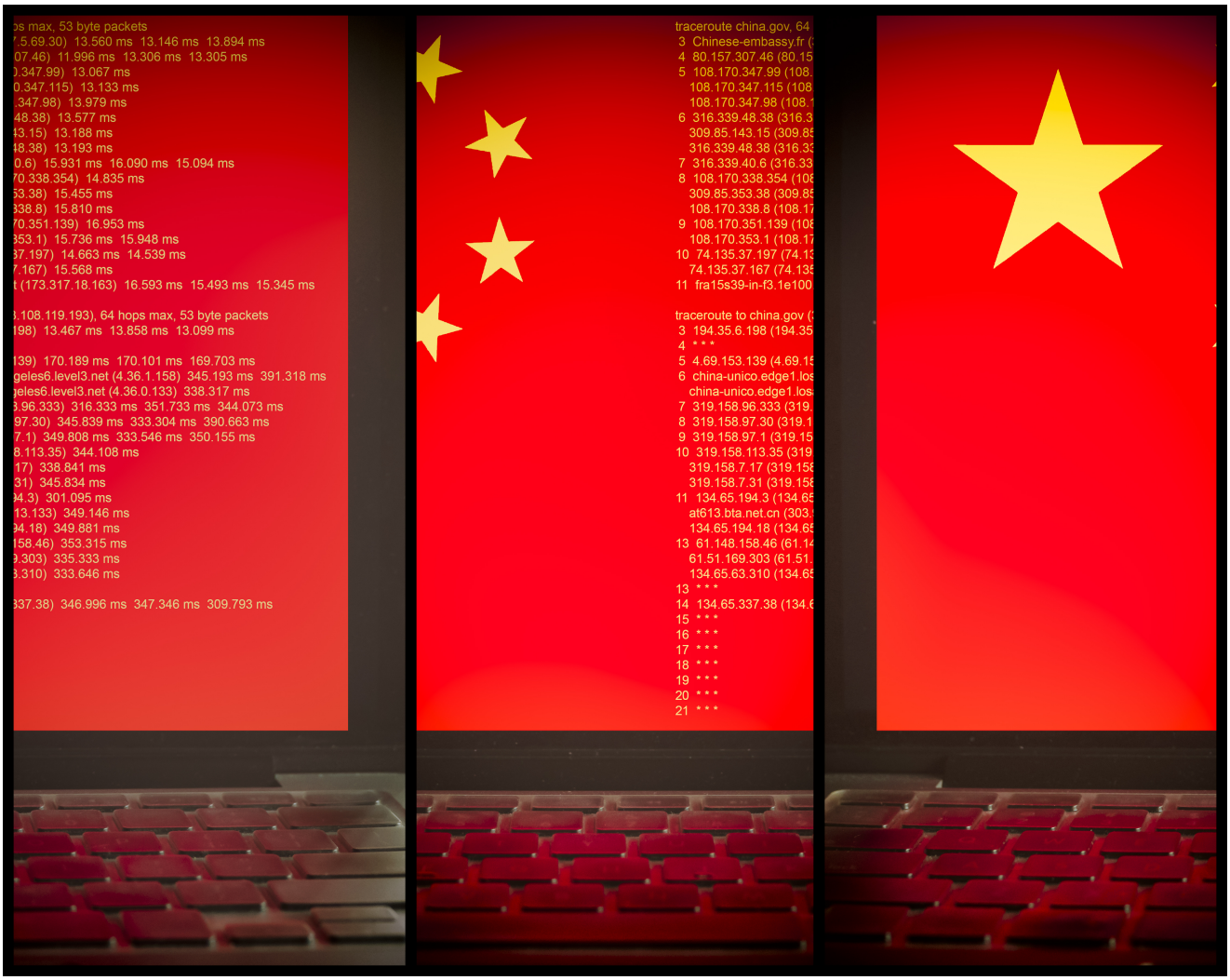
ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape



Back to IronNet Blog

Threat Research

By IronNet Threat Analysis and Research Teams, including lead contributors Morgan Demboski, Joey Fitzpatrick, and Peter Rydzynski



Oct 26, 2021

Editor's note: This post, originally by Adam Hlavek on Jan. 10, 2021, includes updates dated March 1, April 6, 2021, May 28, 2021, and September 7, 2021

1. The latest China cyber attacks

2. Additional China cyber attack threat campaigns by threat actor

The latest China cyber attacks

- APT41's three month attack on Air India
- HAFNIUM attacks on Microsoft Exchange servers
- A new sophisticated backdoor targeting Linux endpoints and servers
- APT31 replicates and uses an NSA Windows-hacking tool known as EpMe
- APT10 conducts sophisticated campaign, known as A41APT, aimed at exfiltrating information from a number of Japan-linked companies in different industry sectors across the world

Over the past two decades, the People's Republic of China (PRC) 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.

On July 19, 2021, the U.S. government and its allies — including the EU, the Five Eyes countries, and NATO — publicly condemned and blamed the PRC for a series of malicious cyberattacks, including the Microsoft Exchange Hacks, global ransomware attacks, and cyberattacks against medical research institutes and universities.

Along with this, the U.S. Department of Justice released an indictment in May (unsealed July 16th) that charged four Chinese nationals with a campaign to hack into the computer systems of dozens of companies, universities, and governmental entities around the world from 2011 to 2018. The nationals are believed to be members of the group tracked as APT40, which is connected to the PRC Ministry of State Security (MSS) Hainan State Security Department (HSSD). The indictment alleges that China has been leading a worldwide hacking and economic espionage campaign, using cyberattacks to steal intellectual property in disregard of bilateral and multilateral agreements.

China targets Taiwanese finance institutions

TLDR: In early February, Symantec released a report detailing a persistent campaign by the Chinese state-sponsored APT Antlion, targeting Taiwanese financial institutions for at least 18 months. In the attacks, the threat actors deployed a backdoor dubbed xPack to maintain extensive access to victim systems, and the primary goal of the campaign is deemed to be espionage as researchers observed the threat actors exfiltrating data from infected networks.

More information: What is notable about the campaign is the extremely long dwell time of many of the compromises that allowed the threat actors ample time for reconnaissance and exfiltration without detection. For example, in one of the undisclosed financial institution's networks, the threat actors spent almost 250 days undetected in the network between December 2020 and August 2021, and spent over 175 days in another victim's network undetected. The initial access vector is reportedly unclear, but researchers believe Antlion exploited a web application flaw to establish a foothold and drop xPack, which is then used to execute system commands, drop additional executables, and stage data for exfiltration. The last activity seen in the campaign was August 2021.

APT15 Campaign Targeting Entities in Over 29 Countries

Microsoft has observed APT15 targeting governments, diplomatic entities, and NGOs in over 29 countries across Central and South America, the Caribbean, Europe, and North America.

Since September 2019, APT15 has conducted activity across several countries, with a large amount of activity targeting Central and South American governments. Using exploits against unpatched systems to compromise remote access services and applications, APT15 leverages credential dumpers or stealers upon intrusion to obtain legitimate credentials, which they use to gain access to victim accounts. APT15 threat actors developed and deployed custom malware that enabled them to maintain persistence on victim networks over extended periods of time. This has allowed it to achieve long-term access to multiple targets, which it uses to perform frequent and scheduled data collection and exfiltration. In the wake of discovering this campaign, Microsoft successfully obtained a court warrant that allowed it to seize 42 domains used by APT15 in the operations.

HAFNIUM Abuse of Log4Shell

Microsoft reports HAFNIUM is exploiting the Log4Shell vulnerability to attack virtualization infrastructure in order to extend their usual targeting.

In these attacks, Microsoft observed HAFNIUM-associated systems leveraging a DNS service typically associated with testing activity to fingerprint systems.

Geopolitical

- Twitter shuts down thousands of state-linked accounts in China that seek to counter evidence of human rights abuses in Xinjiang
- In early December, the U.S. announces a diplomatic boycott of the 2022 Winter Olympics in Beijing, citing “ongoing genocide and crimes against humanity in Xinjiang.”
- China and Japan agree to set up a joint communication hotline by the end of 2022 amid tensions over Taiwan and issues in the East and South China seas.
- In mid-December, U.S. Congress passes a bill called The Uyghur Forced Labor Prevention Act that requires companies to prove that goods imported from China's Xinjiang region were not produced with forced labour.

- Around the same time Congress passes The Uyghur Forced Labor Prevention Act, the U.S. imposes trade restrictions on more than 30 Chinese research institutes and entities over human rights violations and the alleged development of biotechnology to support Chinese military end uses and end users, to include purported brain-control weaponry.

    > The U.S. department of commerce states China "is choosing to use these technologies to pursue control over its people and its repression of members of ethnic and religious minority groups."

- U.S. intelligence agencies state Saudi Arabia is now actively manufacturing its own ballistic missiles with the help of China.

    > The U.S. is now concerned about whether Saudi's ballistic missile advancements could change regional power dynamics and complicate efforts to discuss the nuclear deal with Iran.

TAG-28 attacks on Indian entities

As the bilateral relations between China and India continue to deteriorate over the Line of Actual Control (LAC) dispute in the Galwan Valley, India has become the target of several Chinese state-sponsored cyber attacks. Researchers at Recorded Future [PDF] have identified intrusions targeting Indian entities led by suspected Chinese state-sponsored threat activity group TAG-28. The victims of these intrusions include Indian media conglomerate Bennett Coleman And Co Ltd (BCCL), a multimillion-dollar news organization commonly known as “The Times Group” that consistently reports on the China-India war. It also includes the Unique Identification Authority of India (UIDAI), which contains the biometric data of one billion Indian citizens, as well as the Madhya Pradesh Police Department (MPP), whose Chief Minister was critical of China after the border clashes that occurred in the Ladakh region in June 2020.

In this campaign, TAG-28 used Winnti malware, which is a family of malware that several Chinese threat actors have historically used. In relation to the attack on BCCL, between February and August 2021, four IPs were seen communicating with two Winnti C2 Servers and possibly a Cobalt Strike server, which led to approximately 500 MB of data being exfiltrated from the network. From June 10 to at least July 20, 2021, researchers observed two IPs registered to UIDAI communicating with the same suspected Cobalt Strike C2 server used to target BCCL. Less than 10 MB was egressed from the UIDAI network with an ingress of almost 30 MB, potentially indicating the deployment of additional malicious tooling from the TAG-28 infrastructure. For the targeting of the MPP, the department’s website began communicating with a Winnti C2 server on June 1, 2021. Another MPP IP began talking to the malicious server on July 7 to at least August 9, with around 5MB of data being transferred.

Chinese APTs infiltrate major Afghan telecom provider

Recorded Future's Insikt Group has detected separate intrusion activity linked to 4 distinct Chinese state-sponsored threat actors targeting a mail server of Roshan, one of Afghanistan's largest telecommunications providers. The APTs are RedFoxtrot and Calypso APT, and there are 2 additional clusters using the Winnti and PlugX backdoors that haven't been linked to groups yet. Data exfiltration activity for these intrusions, particularly the Calypso APT activity and the unknown threat actor using the Winnti malware, spiked throughout August and September 2021, which coincided with major geopolitical events like the withdrawal of US troops and the Taliban takeover.

It's not clear from the latest research how the Roshan server was infected, but Chinese APT attacks often begin by exploiting external-facing services or spearfishing campaigns. Roshan offers a hugely valuable platform for strategic intelligence collection, allowing for things like the monitoring of downstream targets, bulk collection of communication data, as well as the ability to track and monitor individual targets. The Chinese government also considers the telecom sector to be of strategic significance in countries participating in the Belt and Road Initiative. So there are many motives here.

Chinese espionage group targets critical infrastructure orgs in Southeast Asia

A Chinese cyber-espionage group has been identified targeting at least four critical infrastructure organizations in a southeast Asian country from November 2020 to March 2021. Organizations targeted include a water company, a power company, a communications company, and a defense organization, and researchers said they found evidence that the attackers were interested in targeting information about SCADA systems.There is evidence that the attacker behind this campaign is based in China, but there is not enough information available to attribute the activity to a known actor. The threat actors made extensive use of living-off-the-land / dual-use tools, including Windows Management Instrumentation, ProcDump, PsExec, and Mimikatz. Espionage seems like the likeliest motive of these attacks, indicated by the activities of credential stealing, lateral movement, and keylogger deployment as well as the types of machines targeted in some of the organizations - most of which were involved in design and engineering. An attacker gaining access to multiple critical infrastructure organizations in the same country could potentially give them access to a vast amount of sensitive information.

DeadRinger Campaign

Security researchers identified three distinct clusters of malicious activities operating on behalf of Chinese state interests, namely Gallium, APT 30/Naikon, and APT27 / Emissary Panda, in a campaign dubbed "DeadRinger." In this campaign, the groups staged a series of attacks that targeted networks belonging to at least five major telecommunications companies located in Southeast Asia from 2017 to at least mid-2021. Researchers assess

that the goal behind these intrusions was to gain and maintain continuous access to telecommunication providers and to facilitate cyber espionage against select targets. In this campaign, there are three observed clusters of activity conducted over various time periods and deploying different malware. Overall, there has been an interesting overlap between these clusters: they were all observed in the same target environment, around the same timeframe, and even on the same endpoints. Overlaps in attacker TTPs across the clusters are evidence of a likely connection between the threat actors, and it is assumed that each group was tasked with parallel objectives in monitoring the communications of specific high-value targets under the direction of a single Chinese body.

SparklingGoblin

ESET researchers recently discovered a new undocumented modular backdoor called Sidewalk, which has been linked to a new APT they are calling SparklingGoblin. SparklingGoblin was first detected in May 2020 by researchers tracking the Winnti group, aka APT41. Even though this campaign exhibited links to Winnti Group, the modus operandi was quite different, leading researchers to start tracking it as a separate threat actor. The new undocumented modular backdoor, Sidewalk, was used during SparklingGoblin's recent campaign targeting a computer retail company in the US. Sidewalk is a backdoor that dynamically loads additional modules sent from its C2 server, uses a Google Docs document as a dead drop resolver, and uses Cloudflare workers web services as a C2 server. SideWalk can collect information about running processes, write received data to file, and call plugins received from the C2 server. SparklingGoblin has been very active from mid-2020 to now and has targeted organizations mostly in East and Southeast Asia, but has targeted a broad range of entities around the world including in the USA.

UNC 215 cyber espionage campaign in Israel

A cyber-espionage group based out of China called UNC215 has been identified conducting a campaign against Israeli government entities, IT providers, and telecommunications companies since January 2019. UNC215 is linked with low confidence to APT27 and is said to target organizations that are of great interest to Beijing's financial, diplomatic, and strategic objectives, demonstrating China's consistent strategic interest in the Middle East related to the Belt and Road Initiative and interest in Israel's robust technology sector. UNC215 has a high level of operational security: it makes a consistent effort to delete tools and any forensic artifacts from compromised systems; uses other victim networks to proxy its C2 instructions in order to evade detection and blend in with normal network traffic; and incorporates false flags. For example, on at least three occasions, UNC215 employed a custom tool leaked from Iranian actors in order to deceive analysts and make it look like Iranian actors were behind the attacks.

HAFNIUM attacks on Microsoft Exchange servers

Dominating the headlines of Chinese cyber attacks is the on-premise Microsoft Exchange server attack, presumed to be carried out by the Chinese APT HAFNIUM. This group has been identified as exploiting Exchange servers through a collection of several zero-day vulnerabilities. The supposed motive behind this attack aligns with the typical strategy of Chinese cyber attacks: intellectual property theft. The four vulnerabilities affect unpatched on-premise Microsoft Exchange servers - versions 2013 to 2019, excluding only Exchange Online (Office365). You can read detailed IronNet analysis and response in our blog "HAFNIUM Targets Microsoft Exchange Zero-Day Vulnerabilities."

LuminousMoth

A Chinese APT, dubbed LuminousMoth by Kaspersky, was discovered spreading fake Zoom software to spy on targets in South East Asia since at least October 2020. The earliest sightings of this currently ongoing campaign were in Myanmar, but the attackers now appear much more active in the Philippines and have an interest in targeting government entities. With activities and tactics appearing to overlap with that of Mustang Panda, LuminousMoth uses two infection vectors in these attacks. The first provides initial access to a system through a spearphishing email containing a DropBox download link. The second infection vector comes after the first has succeeded, in which the malware attempts to spread by infecting removable USB drives. The attackers deploy a post-exploitation tool that impersonates Zoom software with a valid digital signature, using it to scan compromised systems for files with pre-defined extensions that are then copied and transferred to a C2 server. On some compromised systems, the attackers also deployed another post-exploitation tool that steals cookies from a Chrome browser for the purpose of hijacking and impersonating the Gmail sessions of the targets. It is clear that the attacks of this campaign are very large-scale and affect a wide range of targets with the ultimate goal of compromising a few that are of particular interest.

Tag-22

In July 2021, Recorded Future identified a suspected Chinese state-sponsored group tracked as Threat Activity Group 22 (TAG-22) targeting telecommunications, academia, R&D, and government organizations in Nepal, the Philippines, Taiwan, and Hong Kong. The group was first detected in September 2020 targeting a Hong Kong university and airport, but in June 2021, TAG-22 was identified targeting the Industrial Technology Research Institute (ITRI) in Taiwan, Nepal Telecom, and the Department of Information and Communications Technology in the Philippines. In this most recent campaign, TAG-22 used compromised GlassFish servers and Cobalt Strike for initial access before pivoting to Winnti, ShadowPad, and Spyder backdoors for long-term access using actor-controlled C2 infrastructure. Tracked as an independent activity cluster that overlaps with the wider network defined as Winnti Group, TAG-22 leverages shared custom backdoors unique to Chinese state-sponsored groups — including ShadowPad and Winnti — while also using open-source/offensive

security tools like Cobalt Strike and Acunetix. The group's continued use of publicly reported infrastructure indicates that it is experiencing a high degree of operational success despite a range of public reporting regarding its operations.

IndigoZebra

A Chinese APT group dubbed "IndigoZebra" has been identified conducting an ongoing spearphishing campaign against the Afghan government, impersonating the Afghan president as a lure to infiltrate government agencies, leading to the compromise of the Afghan National Security Council (NSC). IndigoZebra has been observed targeting other Central Asian countries as well, including Kyrgyzstan and Uzbekistan, since at least 2014.

In IndigoZebra's infection chain used in its attacks against the Afghan government, the threat actors begin with an email containing a malicious password-protected RAR archive (NSC Press conference.rar), which thwarts some sandbox solutions because it requires user interaction. The RAR archive drops the extracted file (NSC Press conference.exe), which then drops and executes the BoxCaon backdoor (spools.exe). The BoxCaon backdoor, which is a variant of the xCaon malware family, uses Dropbox as a command-and-control (C2) server, sending and receiving commands contained in a specific folder in an attacker-created Dropbox account. The threat actors' use of Dropbox for C2 communications aids in masking the malicious traffic in the victim's network and appears as benign activity in user environments where Dropbox is used (Dropbox comes default on some Windows computers). The backdoor uses a hardcoded access token and has the ability to download, upload, and execute files. Other malware that the group has used in 2020-2021 (primarily against political entities in Kyrgyzstan and Uzbekistan) are hosted on ASN 20473 (CHOOPA) and Vultr - a subsidiary of CHOOPA that is commonly used for malicious purposes by criminals and Chinese APTs.

Linux attacks / RedXOR

In most recent news, a new sophisticated backdoor targeting Linux endpoints and servers was discovered by security researchers at Intezer in early March, and TTPs indicate it is the work of high-profile Chinese threat actors. Dubbed RedXOR, the backdoor masquerades as a polkit daemon (which is a toolkit used for allowing unprivileged processes to communicate with privileged processes), and it is very similar to malware associated with the Winnti Umbrella — a term used to describe a collective of state-backed hacking groups linked to Chinese government interests. The operation is still believed to be ongoing as researchers experienced an "on and off" availability of the C2 server, indicating that the operation is still active. The malware samples were first uploaded from Indonesia and Taiwan— two countries known to be heavily targeted by Chinese APTs. The samples were compiled with a legacy GCC compiler on an old version of Red Hat Enterprise Linux, indicating that RedXOR is used in targeted attacks against legacy Linux systems. It is packaged with the usual suite of tools, including the ability to gather system information, perform file operations, run arbitrary shell commands, and even options to remotely update the malware.

Of note: Victim types and motivations have not been indicated in reports, but the groups that fall under the Winnti Umbrella share an arsenal of malicious tools used in cyber espionage and financially motivated attacks and it has been stated that there has been a large increase in unique Linux malware tools tailored for espionage operations.

Additional China cyber attack 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.

APT31

Overview:

APT31 is a Chinese state-sponsored cyber espionage group focused primarily on acquiring information that can provide political, economic, and military advantages to the Chinese government and state-owned enterprises. Active since at least 2013, APT31 conducts mainly intellectual property theft and espionage operations using a range of tools and techniques to infect target systems, steal credentials, and move laterally within a compromised network. APT31 targets numerous organizations in various sectors, often seeking intellectual property, information that provides a commercial advantage, or sensitive details about government and defense targets of interest.

Recent Activity:

Security researchers uncovered approximately 10 attacks carried out from January to July 2021 by APT31, in which the group used a new dropper and targeted entities in the U.S., Canada, Mongolia, Belarus, and Russia. APT31, also known as Judgement Panda and Zirconium, has been active since at least 2016 and is known to provide data to the Chinese government and enterprises for political, economic, and military advantages. PT Security was able to link these attacks and the new dropper to APT31 because numerous overlaps were found between these malware instances and APT31's DropboxAES RAT trojan in relation to functionality, techniques, and mechanisms used.

On July 21st, the French national cyber-security agency (CERT-FR) warned of an ongoing campaign by Chinese-backed APT31 against a large number of French organizations. CERT-FR investigations show that in these attacks, APT31 compromises routers to leverage them as anonymization relays before carrying out reconnaissance and attack activities. In other words, APT31 uses a network of compromised home routers as operational relay

boxes to gather information and carry out further malicious actions. CERT-FR shared a list of IOCs to help entities assess potential compromises, and more information about the extent of these attacks will likely be made public by French authorities in the near future.

In February 2021, it was reported that APT31 cloned and used a Windows-hacking tool, code-named EpMe, that was originally created by the Equation Group — an APT with links to various branches of the NSA. Essentially, APT31 extracted the core functionality of the tool and created its own replication, known as "Jian" or "double-edged sword," around the exploits included in EpMe. What is concerning (and remarkable) about this reconstructed EpMe tool is that evidence points to the exploit first being used in 2014 — almost three years before it became publicly available with the **Shadow Brokers dump** and was patched by Microsoft.

Jian was first discovered on a U.S.-based network by security researchers at Lockheed Martin, indicating that the tool has largely been used against U.S. targets. Evidence points to the notion that APT31 managed to access both the 32-bit and 64-bit samples of the EpMe Equation Group exploit and replicate them to construct Jian, then using the new version of the exploit alongside their unique multi-staged packer. However, Jian is much less sophisticated than EpMe and it contains many quirks — like support for Windows 2000 even though Windows 2000 was never vulnerable to exploit — indicating that they did not really understand the true nature of the exploited vulnerability and its associated limitations.

The Finnish government officially accused APT31 of hacking into the Finnish parliament in 2020, describing the attack as "aggravated espionage" and "message interception" in order to further Chinese interests. The attack, which led to the compromise of some parliament email accounts, is currently being investigated by the Finnish National Bureau of Investigation (NBI). The threat group has also been accused of targeting the Joe Biden presidential campaign with malicious spearphishing emails that impersonated anti-virus software company McAfee and used legitimate services, like DropBox, in an attempt to steal staffers' credentials and infect them with malware.

Known Targets	Numerous sectors, including legal and consulting, telecommunications, software development, construction and engineering, and aerospace and defense as well as governmental entities in the U.S. and northern European countries, and government and defense supply chain networks

Sample TTPs	• Sophisticated targeted spearphishing • Attacker-controlled URL web beacons sent via email text or attachment • Impersonation of legitimate software, such as McAfee anti-virus software and Oracle, to load malicious code • Leveraging of popular code and file-sharing sites, specifically Github and Dropbox, for their C2 domains to complicate network-based detection • Use of China Chopper webshell for initial compromise and persistence, uploaded to a target web server via a SQL injection or WebDAV vulnerability • DLL search-order hijacking to run a malicious downloader tool (i.e. HanaLoader) that retrieves and runs payloads over HTTPS
AKA	Zirconium, Judgment Panda, Hurricane Panda, BRONZE VINEWOOD, Red Bravo,

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
AKA	Palmerworm, CIRCUIT PANDA

APT 41 / 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 PRC cyber operators, regardless of how specifically each discrete intrusion can be attributed.

Recent Activity:

In June 2021, Mandiant discovered a potential APT41 campaign targeting at least four U.S. state governments in May 2021, in which they used three C2 servers, previously identified malware, and multiple SQL injection attempts. Researchers suspect the group is targeting vulnerable internet-accessible servers of U.S. state government entities to gain initial access for intrusion operations. There is currently an ongoing investigation of these intrusions, so they have not been able to label a specific motive at this time; however, the direct targeting of U.S. state government entities is a concerning development given the nature of APT41 campaigns. This perhaps is an attempt to circumvent better prepared and/or resourced federal agencies and to target state and local government for easier access to the same or similar material.

It was revealed in June 2021 that APT41 is believed to be responsible for an almost three month long cyberattack against Air India. Since at least February 23rd, Group-IB observed an infected device in Air India's network ("SITASERVER4") communicating with a C2 server hosting Cobalt Strike payloads that date back to December 11th, 2020. After this initial compromise, the APT41 threat actors acquired passwords and achieved persistence to move laterally into the larger network with the objective of collecting information inside Air India's local network. Reportedly, at least 20 devices were compromised in the course of this lateral movement, and the attackers managed to use hashdump and mimikatz to exfiltrate NTLM hashes and plain-text passwords from local systems. All in all, APT41 was able to extract almost 24 MB of information from five devices, taking just over 24 hours to spread Cobalt Strike beacons to other systems in Air India's network.

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 Malaysians 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 Malaysian 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 with multiple countries targeted, 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
AKA	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 the PRC 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

AKA	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
AKA	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: see below). 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)
AKA	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:

An A41APT campaign, attributed to APT10, is noted to be a sophisticated campaign that deploys malicious backdoors to exfiltrate information from a number of Japan-linked companies in different industry sectors across the world. The activity was first detected in March 2019, carrying out through December 2020, with latest attacks said to have occurred in January 2021 and JPCERT/CC stating attacks are still ongoing. The campaign includes a multi-stage attack process, with initial intrusion happening via the exploitation of vulnerabilities in Pulse Connect Secure, a widely used SSL-VPN, in order to hijack VPN sessions. In this campaign, APT10 uses previously undocumented malware, most notable of which is one particular piece of malware called Ecipekac, which is a multi-layer loader module used to deliver as many as 3 payloads, such as SodaMaster, P8RAT, and FYAnti. IronNet has created TIRs related to this campaign and pushed them to customer environments.

In addition, 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
AKA	TA429, Menupass, Red Apollo, Stone Panda, Cicada

Collective Defense against China cyber attack threats

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.

About Ironnet

Founded in 2014 by GEN (Ret.) Keith Alexander, IronNet, Inc. (NYSE: IRNT) is a global cybersecurity leader that is transforming how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a number of former NSA cybersecurity operators with offensive and defensive cyber experience, IronNet integrates deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

Back to IronNet Blog