Divided We Hack: Exploring the Degree of Sino-Russian Coordination in Cyberspace During the Ukraine War

Abstract—**China and Russia are arguably NATO's main strategic competitors and potential adversaries. Since 2017, Beijing and Moscow have conducted cyber-espionage operations against NATO members, and the two countries have also reportedly displayed more coordination in the cyber domain. These concerns have become more pressing since the outbreak of war in Ukraine, where multiple sources have shown alleged evidence of Chinese and Russian cyber-operations coordination. While it is commonly accepted that China and Russia cooperate at the strategic level in the cyber domain, this article aims at better understanding whether these two nation-states are also coordinating their affiliated cyber threat groups. We investigate this, drawing on multiple open-access data and sources. Specifically, we empirically examine the activity of three Chinese groups, Mustang Panda, Scarab and Judgment Panda, to assess the presence and degree of coordination with their Russian counterparts. Our analysis shows that, as far as the examined groups are concerned, there was no coordination between Russian and Chinese campaigns, and the latter group sometimes even targeted sensitive Russian civilian and military infrastructures.**

Index Terms—**APT, Cyber Threat Intelligence, Offensive Operations, Ukraine War**

1. Introduction

In April 2022, the British newspaper The Times reported that the day before the Russian invasion in Ukraine (23 February), China-based hackers launched "a huge cyberattack on Ukraine's military and nuclear facilities in the build-up to Russia's invasion". According to the Times, more than 600 websites belonging to Ukraine's defence ministry and other institutions "suffered thousands of hacking attempts" [1]. The Ukraine intelligence services declared they detected hacks that had the attributes of the cyberwarfare unit of the People's Liberation Army [2], [3]. Several researchers and cybersecurity companies have also reported Chinese cyber-activities [4] and raised questions about whether China had advanced notice of Russia's plan in Ukraine, and whether Beijing somehow supported Moscow.

If these hypotheses were confirmed, they would have significant political and military implications. There is extensive literature on the convergence [5], [6] or divergence [7] between the two NATO's strategic competitors and potential adversaries [8]. Their eventual cooperation in cyberspace could strengthen the convergence thesis. From a cyberwarfare point of view, possible coordination between Chinese cyberattacks and Russian cyber and conventional operations would require a fundamental reassessment of the Western strategy and posture in cyberspace [9].

The research question we try to answer with this paper is: "While at a higher strategic level China and Russia are trying to cooperate in the cyber domain, are their affiliated threat groups coordinated and working towards shared goals?" Hence, we explore whether the Chinese and Russian cyber-operations [10] were coordinated and, precisely, whether there are any links between the two countries' military-related Advanced Persistent Threat (APT) activities [11]. We have two goals: first, we investigate, drawing on multiple open-access data and sources, whether there was some form of coordination between Russian and Chinese APTs after the Russian invasion of Ukraine (February-December 2022). Specifically, we focus on three cases allegedly involving groups linked to Beijing: Mustang Panda, Scarab and Judgment Panda. Our analysis suggests a more nuanced picture than is commonly depicted in the public debate. Namely, despite sometimes sharing the same military targets, China and Russia maintain very different and sometimes divergent goals in cyberspace. In this way, we aim to provide an empirical contribution to the literature on offensive cyber operations. Second, and related, we focus on the implications that the presence or absence of Russian-Chinese coordination entails for our understanding of coordinated efforts of nation-states in cyberspace and, more broadly, the role of coordinated or uncoordinated cyber offensive operations. Our analysis shows the structural difficulties in coordinating to launch APTs with shared objectives. Cooperation between Russia and Chinese APTs in Ukraine would have to involve the transfer of knowledge, resources and a level of sophistication that makes it extremely difficult even if Beijing and Moscow's strategic goals would become more aligned in the medium or long term. We suggest that the structural characteristics of cyber offensive operations, by their nature, limit coordination in cyberspace.

2. Cyberattacks in Ukraine: a possible Moscow-Beijing connection?

Even before the Russian invasion, there were significant concerns about possible Russian cyberattacks paralysing Ukraine and "create shock and awe, causing Ukraine's defences or will to fight to collapse" [12], [13]. Specialised investigations during the first ten months of the war showed that cyberattacks had a limited effect on the battlefield [14], but played an active role in gathering information and causing damage to Ukrainian critical infrastructure [15]–[18]. For instance, state-sponsored

APTs (Advanced Persistent Threats) [19] have at times operated in support of Russian kinetic operations; other times, they were used to infiltrating Ukrainian government agencies, secure footholds in critical infrastructures and reduce the Ukrainian public's access to information [17], [20], [21]. Since the beginning of the conflict, there have been rumours about the possible involvement of Beijing-connected groups in launching several APTs against Ukrainian political and military targets. According to Check Point Software Technologies, an Israeli security company, the frequency of cyberattacks from Chinese IP addresses around the world increased by 72% in the week from March 14 to March 20, compared with the seven days before Russia's invasion of Ukraine began [22]. This created concerns, both in the media and among Western observers and policymakers, that there was some form of coordination between Chinese and Russian groups and authorities [23]. After all, the two countries have a long history of cooperation in cyberspace [24]. In 2009, China and Russia signed an information security agreement in the framework of the Shanghai Cooperation Organization. In 2015, Russia and China signed an agreement to create contact points and communication channels between various government entities to realise joint scientific projects in cyberspace [25]. The two countries also worked together to promote the notion of "cyber sovereignty" in international organizations [26]. This created concerns about possible structured cooperation between the two countries in cyberspace [27]. Until the invasion of Ukraine in 2022, however, scholars and observers agreed that coordination between the two countries had been confined to declaratory policy positions rather than actual coordination on the ground. Reports of a possible Chinese cyber-attack before the Russian invasion in February 2022 and the rumours about Beijing-connected groups active in Ukraine, however, make it necessary to explore whether there is any form of coordination between Chinese and Russian groups in Ukraine.

3. Research Design and Methodology

There are two methodological levels in this paper precisely because the purpose of this work is twofold: first, to analyse in detail - including a technical perspective - APT activity in which there is alleged Chinese involvement, and second, based on this analysis, to evaluate whether there was coordination between Chinese and Russian groups. In this paper, we have established our methodological approach on several pillars. The first is founded on competing interests: APTs are often state-sponsored and driven by geopolitical interests. As a result, different APTs may have conflicting goals or objectives, which may hinder their ability to coordinate with each other. Then there is operational security: APTs often operate secretly and may not trust each other. Sharing information or coordinating activities can put their operations at risk and compromise their ability to conduct successful attacks. Given the clandestine nature of their operations, the latter has a low level of coordination by definition. APTs may not trust each other: APTs are complex operations that require significant resources, including human capital, finance and technology. The coordination of these resources across multiple groups and levels can be challenging and can only sometimes lead to results of real collaboration between the parties involved. Finally, there are plenty of communication barriers: APTs can operate with different languages or operate in different time zones, making coordinating activities or sharing information difficult. A potential methodological misconception that could apply to the study of the cooperation between different APTs is to assume that all APTs are part of a more significant coordinated effort. This misconception may stem from APTs often using similar tactics and techniques, such as spear phishing attacks, social engineering, or zero-day exploits. Consequently, a central coordinating body must be behind these attacks. However, the reality is often more complex, and many APTs operate independently or in small groups, with little or no coordination with other threat actors. In this paper, we adopt a different research approach to understand the need for more cooperation between different APTs. Thus, we investigate three case studies: Mustang Panda, Scarab and Judgment Panda. These are relevant because they were among the most significant APTs carried out since the outbreak of the Russo-Ukrainian war, and multiple sources have indicated the possibility of coordination between Russia and China. These three groups were chosen for their relevance to the period we chose to analyse and for the breadth of publicly available and scrutinised information available from the beginning of the Russian-Ukrainian conflict to the end of 2022.

It is important to underline is that, in the context of cyberspace, we believe that cooperation and coordination are entirely different concepts. Cooperation refers to sharing resources, information, or skills to achieve common goals or tackle shared challenges. Coordination refers to the organization of the efforts of the various actors, in particular of the different APTs, aimed at ensuring the efficient and effective achievement of the shared objectives. While cooperation represents a willingness to work together, coordination focuses on managing and aligning those efforts to maximize efficiency.

To collect the data, we first used CTI databases made available by Mandiant, such as Mandiant Advantage. While Mandiant Advantage can provide valuable information about APTs, it is not specifically designed to analyse the degree of coordination between different APT groups. However, the platform offers valuable insights. First and foremost, it allowed us to find threat groups belonging to China and Russia, and since Mandiant shows the degree of confidence in each attribution to a specific country, we were able to work only on APTs with ”almost certain” attribution [28]. Additionally, by analysing data available on the platform, such as the tactics, techniques and procedures (TTPs), infrastructure, timestamps of known attacks, and other indicators of compromise (IOCs) associated with Russia- and China-related APT groups, we identified similarities or differences that noted a lack of coordination or cooperation between these different APT groups. Additionally, by monitoring the goals and targets of these APT groups, we identify instances where they pursue conflicting or competing goals. To do this, we rely on specific methodological frameworks, such as the F3EAD intelligence cycle, commonly used within Western militaries. The F3EAD intelligence cycle is a process used to collect and analyse intelligence supporting military operations. It consists of six steps: Find, Fix, Finish, Exploit, Analyse and Dissemination. If applied to the study of APTs, the F3EAD cycle can provide a valuable framework for understanding whether there is, in fact, cooperation between the APTs of Russia and China. Here is a brief description of each cycle phase:

1) Find: The Find stage involves identifying potential targets or sources of information.
2) Fix: The Fix step involves gathering more detailed information about the target.
3) Finish: The Finish phase provides for the neutralisation of the target.
4) Exploit: The Exploit phase involves collecting any information or material in the target site that may have intelligence value.
5) Analysis: The analysis phase involves analysing the information collected to identify patterns, connections and other valuable information for future operations.
6) Dissemination: The dissemination phase involves sharing information with relevant staff and decision-makers.

Applying the F3EAD to our research meant finding the most suitable threat groups to study, then collecting as much data as possible on them - both on the previously mentioned CTI platforms and on open source resources such as those presented below -, then analysing all the retrieved information to understand their behaviour, goals, and procedures, all in order to assess the presence and degree of cooperation between the chosen Chinese groups and their russian counterparts.

Competing interests, operational security concerns, and legal constraints that hinder coordination between APTs can also make gathering and analysing information about these adversaries difficult. However, using the F3EAD cycle to gather and analyse intelligence, it is possible to identify shared TTPs used by different APTs, which can help build a more comprehensive understanding of the threat and develop effective countermeasures. By applying this methodology, we can better understand the need for more cooperation between Chinese and Russian APTs. Through the following framework, the resulting analysis shows us that APTs have different motivations, goals and operational objectives that make cooperation difficult or unlikely, further revealing that these APTs engage in aggressive operations against each other, leading to a lack of trust and willingness to cooperate.

The collection of OSINT on APTs also helped assess the lack of cooperation between different APTs for several reasons. OSINT sources, such as social media platforms, public forums, blogs, and news articles, provided additional information about APT activities that were unavailable in the examined CTI databases. It provided information about APTs TTP, objectives, goals, and motivations. OSINT is undoubtedly valuable for understanding the threat landscape by providing a broader perspective on the motivations, capabilities and strategies of different APTs. Using OSINT also helps identify information gaps and highlight areas for further research. It can inform the collection of additional information and help refine the analysis of APT activities. Overall, OSINT´s collection and analysis of APTs can provide valuable insight into the need for more cooperation between different APTs.

Finally, we integrate the information and data obtained from the previously mentioned CTI platforms with the MITRE ATT&CK framework, the Malware Information Sharing Platform or MISP, and Yara rules, which proved valuable tools for understanding the lack of cooperation and coordination between different APT groups. Specifically, the MITRE ATT&CK framework provides a comprehensive taxonomy of TTPs. The MISP is an open-source platform for sharing threat intelligence data between organisations. By analysing MISP data, it is possible to identify patterns of activity that suggest a lack of coordination between different APT groups. For example, if two APT groups are targeting the same organisation or industry using similar TTPs they need to share infrastructure or collaborate in some way, if they don't, it could just indicate a lack of coordination or communication between the groups. Yara rules provide a type of pattern-matching method used to identify malware and other threats based on specific behaviour patterns or characteristics. By creating and sharing Yara rules that target specific APT groups, researchers can more effectively detect and monitor the activities of these groups. By analysing Yara rule matches, we can identify patterns of actions that could suggest a lack of coordination between different APT groups. For example, if two APT groups use additional malware detected by different Yara rules, it could indicate a lack of coordination.

Collectively, the MITRE ATT&CK framework, MISP, and Yara rules proved to be powerful tools for understanding the lack of cooperation and coordination between different APT groups. However, it is essential to note that APT groups are often highly sophisticated and adaptive and may use tactics to avoid detection or mislead researchers. Therefore, additional care and a rigorous methodology were used to support the analysis with these tools.

MITRE ATT&CK navigator tables for the three APTs being analysed are given in the Appendix of this document as a quick reference to their TTPs.

4. Mustang Panda

Mustang Panda, also known as “RedDelta” or “Bronze President” [29], is a Chinese-connected threat actor allegedly responsible for targeting non-governmental organisations with a specific focus on Asian countries. In July 2021, the Slovak cybersecurity company ESET noted malicious activities linked to Mustang panda targeting through a remote access tool known as PlugX, research entities, internet service providers and diplomatic missions based in Eastern Europe [30]. ESET's findings aligned with public disclosures from Google's Threat Analysis Group (TAG), which revealed that “the targeting of European organisations has represented a shift from Mustang Panda's regularly observed Southeast Asian targets” [31]. Shortly before and shortly after the Russian invasion of Ukraine, Proofpoint, a California based security vendor, noted increased activity from a group known as RedDelta, previously linked to Mustang Panda, as some researchers believed they were part of the same group [32]. In its report, Proofpoint emphasises that “the operational tempo of these campaigns, specifically those against European governments, have increased sharply since Russian troops began amassing on the border of Ukraine" [33]. The malicious file used for the phishing attack came with the title, "Situation at the EU borders with Ukraine.zip," indicating Google and Proofpoint were witnessing the same activity. Our analysis of TTPs shows that, commonly to other APTs, Mustang Panda uses commodity solutions for file hosting and sending emails, e.g. using Dropbox to collect their malicious payloads and employing SMTP2GO for their phishing campaign emails. Before the operation, Mustang Panda strived to have direct control over the necessary infrastructure, e.g. by purchasing all the domains required by their C2 (Command & Control) chain well in advance. Initial access is usually obtained by phishing emails with malicious links and/or attachments. The execution of malicious code is performed via several means: Mustang Panda is known for using WMI (Windows Management Instrumentation), PowerShell, Command Shell, Visual Basic, Word documents macros, and, in some cases, Windows Scheduled Tasks. Scheduled Tasks is also used to obtain persistence and privilege escalation, in addition to other techniques such as DLL (Dynamic Link Library) side-loading and, once again, the exploitation of WMI. Defence evasion techniques range from very basic to more advanced ones. The former include hiding, renaming, or having double extensions on a file. For instance, a file named "adobeupdate.dat" was used to disguise PlugX, and a file named OneDrive.exe was used to disguise a CobaltStrike payload. The latter involved more complex tools such as InstallUtils and MSHTA in launching scripts and executing stages. Credential access happens via hash extraction from volume clones of NTDS.dit files, a database at the very core of Active Directory containing information about users, principals, and groups. The discovery of tactical goals is usually achieved by looking for documents via standard searches. Network configuration and layouts are found via common CLI commands such as ipconfig and netstat -ano. The same goes for process discovery, which is usually done by task list commands. One of the most peculiar techniques used by Mustang Panda is that to achieve lateral movement, removable media, such as USB connections, are used. Data collection usually happens with batch scripts; data is then RC4 encrypted and archived under password protection. RC4 encryption is also employed in C2 communication via common HTTP methods, such as POST. Mustang Panda is also known for being able to exfiltrate data from air-gapped networks via removable media, such as USB drives.

The sophisticated TTPs used by Mustang Panda made it extremely unlikely that heterogeneous groups such as the Chinese and Russian hackers could operate in a coordinated way. The lack of coordination between Russian and Chinese groups also seems to be confirmed by Mandiant's data, which notes that Mustang Panda was targeting Eastern European countries, including Ukraine, well before the Russian invasion. Moreover, no significant links or coordination activities have been identified between this threat actor, which Mandiant traces as (uncategorized) UNC3716, and the other Russian APTs on the Ukrainian front [34]. Most importantly, while Mustang Panda was targeting Eastern Europe and Ukraine, we observed the activities of the Chinese group against Russian targets. The malicious executable carrying PlugX was included in a report on the border detachment in Blagoveshchensk, a city of strategic importance for Russia, located on the Sino-Russian border, called "Blagoveshchensk - Blagoveshchensk Border Detachment [.] Exe". The filename was chosen to target military officials and personnel familiar with the region. That executable, which appeared to be a legitimate document that used a PDF icon, once opened, distributed the malware PlugX.

Mustang Panda's goal seems to be to take advantage of the war between Ukraine and Russia to be able to acquire sensitive economic and military information from both sides. Indeed, the most common file types exfiltrated by Mustang Panda in attacks targeting Russia are Microsoft Office documents (.docx, .xlsx, .pptx, etc.), PDF documents and plain text files. Other exfiltrated file types include audiovisual data in various forms, including audio recordings (.mp3) and images (.jpg, .png, etc.) or drawings. Emails, including entire conversations, are also exfiltrated. This APT also tries to collect data from browser profiles from various web browsers such as Chrome, Firefox, Opera and more. Susceptible data is collected from the victims' computers, and, in most cases, these are computers used by the government, the state administration, the police, and the army.

5. Scarab

U.S. security company SentinelOne identified one of the hacker groups Scarab, allegedly linked to the Chinese government, as particularly active both before and after the Russian invasion of Ukraine. SentinelOne's analysis follows notice #4244 from the Ukrainian Computer Emergency Response Team (CERT-UA) in mid-March, revealing indicators of a threat actor dubbed UAC-0026 and that CERT-UA has linked to Scarab APT [35]. The email may have been created on a computer using the Chinese language, according to SentinelOne. Tom Hegel, the company's senior threat researcher, said the attack by Scarab "represents the first publicly reported attack on Ukraine from a non-Russian [Advanced Persistent Threat]" [36]. As of November 2022, there is little public and documented information available on Scarab [37]. This makes a complete analysis of all MITRE ATT&CK tactics particularly difficult. Reconnaissance-wise, this APT is only known for using commodity passive and active information-gathering tools. There is no documented use of bespoke, custom tools for this purpose. Regarding resource development, it has been observed that this actor has been reusing many loaders, malwares, and C2 infrastructures over the years. This reuse of resources led researchers to attribute with high confidence the recent attacks in Ukraine, named UAC-0026, to the group known as Scarab. Initial access is obtained mainly by phishing and spear-phishing campaigns that use malicious attachments with titles carefully tailored to their targets. For example, in the March 2022 attack against Ukraine, documented by the Ukrainian CERT, a .rar file named "On the preservation of video recordings of the criminal actions of the army of the Russian Federation.rar" was used as a lure document. Interestingly, this last document metadata reveals that the file was created in a Windows environment with a Chinese locale, for the file's author is the Chinese Windows default "用户" (yònghù - user). This specific attack against Ukraine is also a prime example of how this group executes malware and gains persistence. The aforementioned .rar file contains an .exe file with a similar name. Once this file is executed, three things happen. First, a decoy PDF document is shown to the user, while a malware named HeaderTip is run, and persistence is ensured by adding to the registry an Autorun Key. In the past, Scarab used to employ two backdoors in succession, first, a simpler one, dubbed "Scieron", which would install the more complex one, "Scieron B", a more advanced backdoor with a rootkit-like component. This advanced backdoor was able to open shells, manage processes, files and directories, and edit registry entries. At the same time, the rootkit-like component would allow hiding some of the malware network activity happening over TCP. Scieron might be the predecessor of HeaderTip, as they share many common patterns, for instance, both leverage DLL loading for code execution and defence evasion. As mentioned earlier in the paper, Command and Control most often happens via DDNS, and partly via common HTTP methods [38].

Again, there are no indications of coordination between Russian and Chinese groups. While the public news has attributed the activity of HeaderTip to actors linked to China, Mandiant has yet to make a definitive attribution on the origin of this intrusion and currently attributes UNC532 with little confidence to the Chinese actor APT5. Based on the objectives known since the beginning of the Ukrainian invasion, and not just those carried out on Ukrainian soil since March 2022, HackerNews assesses with moderate confidence that Scarab will operate to gather militarily sensitive information [39].

6. Judgement Panda

Between March and April 2022, Google revealed that it had warned the US government about a phishing attack conducted against Gmail users in Eastern Europe by a Chinese-backed hacking group APT31, also known as "Zirconium" or "Judgment Panda" [40]. This group, active for many years, specialises in intellectual property theft and cyberespionage, often against non-governmental entities and private actors.

Judgment Panda groups use standard commodity tools for both active and passive reconnaissance. It is also well known that Judgment Panda widely employs phishing and spear-phishing techniques via email [39]. Regarding resource development, Zirconium is known for purchasing the domains needed for their operations and for using standard file-hosting websites to store their malware, for instance, employing distributed source code management websites such as GitHub. Initial access is obtained via phishing and spear-phishing emails containing malicious links and web beacons. Windows Command Shell and Python scripts are used to execute code once initial access has been achieved. The APTs launched by Judgment Panda have a peculiar way of obtaining persistence: they create a Registry Run key named "Dropbox Update Setup" that runs a malicious Python binary. The binary mentioned above is also - sometimes - used to achieve privilege escalation. The exploit of CVE-2017-0005 is another well-known technique, and this APT uses it to gain unintended, additional privileges. The same fake Registry Run key can also be considered a blatant defence evasion. Concurrently, Judgment Panda also employs other means to evade defences, for instance, by encrypting exploit code and payloads with AES256 (and employing a SHA1-derived decryption key) and by using the msiexec.exe command line utility to launch malicious MSI files. As far as credential access is concerned, there is little data available. The only documented technique known is that this APT can retrieve credentials from browsers like MSIE and Chrome [41]. The main discovery objectives of Judgment Panda are related to the system time, network settings, proxy server configurations, and system architecture. These are all used, at a later date, for C2 communication. Most of the communication within the C2 is JSON-based, encrypted with AES256. There is evidence of them leveraging Dropbox APIs for their Communication and Control efforts. The same communication line with Dropbox allows for exfiltrating data, one commodity tool to rule them all. No publicly documented information exists on how this APT performs the lateral movement.

There is little evidence of coordination between Judgment Panda and the APTs launched by pro-Russian groups. The Google Threat Analysis Group noted in particular that APT31, despite having carried out reconnaissance actions in Eastern Europe and Ukraine, has also targeted government organisations and the military in Russia. In April 2022, using Yandex.Disk as a C2 server to masquerade, APT31 allegedly attacked several Russian energy and media companies through a malicious document. Malware analysis showed that Judgment Panda was behind the attacks: both campaigns in Eastern Europe and Russia contained identical snippets of code to collect information about network adapters and collect data on the infected system; the document stubs bore apparent similarities. In both cases, cloud servers were used to control the malware.

Some analysts and experts have noted that Russian cybercriminals, using hacking forums such as "RAMP" and "XSS", have tried to involve their Chinese counterparts in conversations to collaborate in common cyber-attacks. In a 2021 Flashpoint report, it was highlighted that the RAMP forum had seen at least 30 new registrations of Chinese users [42]. However, it should be noted that, based on previous observations, this could be a misinformation activity. The RAMP forum was created in July 2021 to allow different hackers to openly discuss ransomware-related tools, following the ban on ransomware-related topics on several clandestine forums. Already in October 2021, the administrator of RAMP "Orange" ("boriselcin"), who also managed the website "Groove", published a post asking Chinese threat actors to attack the United States. After the post received media attention, "Orange" claimed that the operation was only launched to manipulate the media and researchers. Mandiant often observes that threat actors from different countries collaborate on clandestine forums. It is undoubtedly true that expanding recruitment to incorporate actors from other regions can improve overall group skills as members can share tactics, tools, malware and methods. However, it is difficult to observe any coordination between Russian and Chinese-associated cyber groups in the case of Judgment Panda.

7. Conclusions

Although media outlets and some observers have hypothesised forms of coordination between APTs conducted by pro-Chinese groups and Russian cyber and kinetic operations, our analysis shows no evidence to support this argument [43]. Through a detailed investigation of three APTs active in Eastern Europe and allegedly conducted by Chinese hacker groups - Mustang Panda, Scarab and Judgment Panda - we uncovered both the technical characteristics of these cyberattacks and their possible links with Russian APTs. Regarding techniques, we observe that these APTs mainly adopt commodity tools and various sophisticated techniques, and try to obtain information from their intended targets through reconnaissance, initial access, execution, persistence, privilege escalation, credential access, and lateral movement [44]. Seldom have these APT groups been found to develop completely new custom-made tools. Regarding the connection with Russian groups, we have seen that the behaviours of these APTs are to target both Ukrainian and Russian political and military objectives and, conceivably, seek to exploit the war (and the confusion generated by it) to gather sensitive information from both sides.

Our paper has substantial politico-military implications. Our analysis strengthens the thesis of structural divergence between China and Russia. The examined pro-Chinese groups have sensitive Russian information among their primary targets. We also highlight the difficulties in coordinating offensive cyber operations. Coordination in cyber operations implies the transfer of knowledge and resources and a high level of sophistication. APTs, by their very nature, require very close cooperation between those actors who carry them out, which is not easy to achieve between hacker communities with different modus operandi, and behaviours, different forums, payment methods, codes of conduct and values [45].

Moreover, on a technical level, cooperation between APTs would require sharing the operation's preparatory and command and control infrastructure. These include domain names of phishing sites, leaked email addresses and the infrastructure which remotely operates to maintain communication with compromised systems within a target network. The preparatory infrastructure concerns the tools used to get into a state of readiness to conduct information operations and includes databases used for target mapping. Rarely, an attacker dismantles this infrastructure [46] after a (failed) operation, so a state or a hacker group has no incentive to share it with other parties. Another obstacle to cooperation at the technical level between APTs would be the nightmarish complexity of integrating code and software written by different and heterogeneous groups due to the different development methodologies, coding styles, polyglot environments, and strict need-to-know requirements. To summarise, then, based on the examined threat groups, it would seem highly challenging to achieve, in the cyber domain, the level of coordination between different actors to which we are accustomed in other domains, such as that of kinetic military operations, even when countries with shared strategic goals are involved.

Based on these considerations, our paper can open up interesting avenues for research. From a scholarly point of view, coordination, as a behaviour, in offensive cyber operations should be further investigated. Other studies have shown the difficulties in transferring cyber-arms and cyber commands due to the transitory nature of cyberweapons [47]. Future research may extend this argument by looking at how the structural characteristics of APTs create constraints to cooperation in cyberspace. If true, Western states and organisations might worry less about joint cyber-offensive operations against their strategic targets and focus on other threats.

From an empirical perspective, our analysis shows that combining technical tools and databases and systematic cross-checks of open-source information can lead to detailed analyses of APTs and a better understanding of offensive cyber operations. This methodological toolkit allows scholars and analysts gain insights on complex and multi-faceted phenomena such as APT modus operandi and behaviour. Moreover, it can help public and international organisations like NATO or the EU and Western states better protect themselves against malicious cyber-activities.

References

[1] M. Tucker, "China accused of hacking Ukraine days before Russian invasion," *The Times*, Mar. 2023. [Online]. Available: https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf

[2] K. Tanmay, "DECODED - Did China Help Moscow Hack Ukraine & Share Critical Intelligence Before The Russian Invasion?" Apr. 2022. [Online]. Available: https://eurasiantimes.com/decoded-did-china-help-moscow-hack-ukraine-russian-invasion/

[3] I. Kagubare, "Ukraine intelligence accuses China of hacking days before invasion: report," Apr. 2022. [Online]. Available: https://thehill.com/policy/cybersecurity/3256792-ukraine-intelligence-accuses-china-of-hacking-days-before-invasion-report/

[4] G. Corera, "Mystery of alleged Chinese hack on eve of Ukraine invasion," Apr. 2022. [Online]. Available: https://www.bbc.com/news/technology-60983346

[5] R. K. Perizat, "China and Russia: between partnership and competition," Jan. 2022, section: EDITORIALS. [Online]. Available: https://theasiatoday.org/editorials/china-and-russia-between-partnership-and-competition/

[6] P. Stronski and N. Ng, "Cooperation and Competition: Russia and China in Central Asia, the Russian Far East, and the Arctic." [Online]. Available: https://carnegieendowment.org/2018/02/28/cooperation-and-competition-russia-and-china-in-central-asia-russian-far-east-and-arctic-pub-75673

[7] J. Srinivas, "Russia and China in BRICS: Convergences and Divergences," in *Future of the BRICS and the Role of Russia and China*, J. Srinivas, Ed. Singapore: Springer Nature, 2022, pp. 147–192. [Online]. Available: https://doi.org/10.1007/978-981-19-1115-6_5

[8] R. J. Harknett and M. Smeets, "Cyber campaigns and strategic outcomes," *Journal of Strategic Studies*, vol. 45, no. 4, pp. 534–567, Jun. 2022, publisher: Routledge _eprint: https://doi.org/10.1080/01402390.2020.1732354. [Online]. Available: https://doi.org/10.1080/01402390.2020.1732354

[9] L. Kello, "Cyber Disorders: Rivalry and Conflict in a Global Information Age." [Online]. Available: https://www.belfercenter.org/publication/cyber-disorders-rivalry-and-conflict-global-information-age

[10] M. D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," no. 42, 2013. [Online]. Available: https://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf

[11] J. R. Lindsay, T. M. Cheung, and D. S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press, May 2015. [Online]. Available: https://doi.org/10.1093/acprof:oso/9780190201265.001.0001

[12] W. Courtney and P. A. Wilson, "If Russia Invaded Ukraine," Dec. 2021. [Online]. Available: https://www.rand.org/blog/2021/12/expect-shock-and-awe-if-russia-invades-ukraine.html

[13] G. Keir, "Putin does not need to invade Ukraine to get his way," Dec. 2021. [Online]. Available: https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way

[14] J. Vicic and R. N. Metha, "Why Russian Cyber Dogs Have Mostly Failed to Bark," Mar. 2022. [Online]. Available: https://warontherocks.com/2022/03/why-cyber-dogs-have-mostly-failed-to-bark/

[15] M. Miller, "Russian invasion of Ukraine could redefine cyber warfare," Jan. 2022. [Online]. Available: https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051

[16] P. Carly, "US, UK and EU blame Russia for 'unacceptable' Viasat cyberattack | TechCrunch." [Online]. Available: https://techcrunch.com/2022/05/10/russia-viasat-cyberattack/

[17] "An overview of Russia's cyberattack activity in Ukraine," Microsoft, Tech. Rep., 2022. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[18] J. Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications." [Online]. Available: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657

[19] "Advanced Persistent Threat - Glossary | CSRC." [Online]. Available: https://csrc.nist.gov/glossary/term/advanced_persistent_threat

[20] A. Scroxton, "Mandiant analysts: Russia-backed APTs likely to ramp up attacks | Computer Weekly." [Online]. Available: https://www.computerweekly.com/news/252512299/Mandiant-analysts-Russia-backed-APTs-likely-to-ramp-up-attacks

[21] ——, "Russia-linked APTs targeted fleeing Ukrainian civilians | Computer Weekly." [Online]. Available: https://www.computerweekly.com/news/252522996/Russia-linked-APT-targeted-fleeing-Ukrainian-civilians

[22] G. McDougall, "Cyber Attacks on NATO Countries Surge by 116%," Mar. 2022. [Online]. Available: https://blog.checkpoint.com/2022/03/21/cyber-attacks-from-chinese-ips-on-nato-countries-surge-by-116/

[23] Y. Wei, "China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty," Jun. 2016, section: Feature. [Online]. Available: https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/

[24] A. Gilli and M. Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security*, vol. 43, no. 3, pp. 141–189, Feb. 2019. [Online]. Available: https://doi.org/10.1162/isec_a_00337

[25] "Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development," Mar. 2023. [Online]. Available: http://en.kremlin.ru/supplement/5770

[26] D. Bandurski, "China and Russia are joining forces to spread disinformation," Mar. 2022. [Online]. Available: https://www.brookings.edu/techstream/china-and-russia-are-joining-forces-to-spread-disinformation/

[27] K. Jackson Higgins, D. R. February 09, and 2016, "Chinese Cyberspies Pivot To Russia In Wake Of Obama-Xi Pact," Feb. 2016, section: endpoint. [Online]. Available: https://www.darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact

[28] S. Kent, "Words of Estimative Probability," 1964. [Online]. Available: https://catalog.archives.gov/id/7282770

[29] "Mustang Panda, TA416, RedDelta, BRONZE PRESIDENT, Group G0129 | MITRE ATT&CK®." [Online]. Available: https://attack.mitre.org/groups/G0129/

[30] A. Côté Cyr, "Mustang Panda's Hodur: Old tricks, new Korplug variant," Mar. 2022, section: ESET Research. [Online]. Available: https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/

[31] S. Huntley, "An update on the threat landscape," Mar. 2022. [Online]. Available: https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/

[32] "Chinese State-Sponsored Group 'RedDelta' Targets the Vatican and Catholic Organizations," *Recorded Future*, 2020. [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf

[33] M. Raggi, "The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates | Proofpoint US," Mar. 2022. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european

[34] D. Bienstock, M. Derr, J. Madeley, T. McLellan, and C. Gardner, "UNC3524: Eye Spy on Your Email." [Online]. Available: https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

[35] T. Hegel, "Chinese Threat Actor Scarab Targeting Ukraine," Mar. 2022. [Online]. Available: https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/

[36] A. Teraoka, "Chinese hackers launch cyberattacks against Ukraine amid war." [Online]. Available: https://asia.nikkei.com/Politics/Ukraine-war/Chinese-hackers-launch-cyberattacks-against-Ukraine-amid-war

[37] Y. Li, "Scarab attackers took aim at select Russian targets since 2012." [Online]. Available: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8bfa7311-fdd9-4f8d-b813-1ab6c9d2c363&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[38] "CVE - CVE-2017-0005." [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0005

[39] L. Ravie, "Another Chinese Hacking Group Spotted Targeting Ukraine Amid Russia Invasion," section: Article. [Online]. Available: https://thehackernews.com/2022/03/another-chinese-hacking-group-spotted.html

[40] M. Kaminska, J. Shires, and M. Smeets, "Tallinn Workshop Report," 2022.

[41] S. Gatlan, "Microsoft: State-backed hackers are targeting the 2020 US elections." [Online]. Available: https://www.bleepingcomputer.com/news/security/microsoft-state-backed-hackers-are-targeting-the-2020-us-elections/

[42] S. Wadhwani, "Russian Darknet Forum RAMP Reemerges With Chinese-speaking Hackers At the Wheel." [Online]. Available: https://www.spiceworks.com/tech/security/news/russian-darknet-forum-ramp-reemerges-with-chinese-speaking-hackers-at-the-wheel/

[43] B. Toulas, "Russian ransomware gangs start collaborating with Chinese hackers." [Online]. Available: https://www.bleepingcomputer.com/news/security/russian-ransomware-gangs-start-collaborating-with-chinese-hackers/

[44] G. Austin, K. Lin Tay, and M. Sharma, "Great-Power Offensive Cyber Campaigns: Experiments in Strategy," Tech. Rep. [Online]. Available: https://www.iiss.org/blogs/research-paper/2022/02/great-power-offensive-cyber-campaigns

[45] W. DeSombre and D. Byrnes, "Thieves and Geeks: Russian and Chinese Hacking Communities," 2018. [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2018-1010.pdf

[46] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," 2011.

[47] M. Smeets, "Cyber Arms Transfer: Meaning, Limits, and Implications," *Security Studies*, vol. 31, no. 1, pp. 65–91, Jan. 2022, publisher: Routledge _eprint: https://doi.org/10.1080/09636412.2022.2041081. [Online]. Available: https://doi.org/10.1080/09636412.2022.2041081

A. MITRE ATT&CK Techniques used by the analysed threat groups

TABLE 1: JUDGMENT PANDA TECHNIQUES

ID	NAME	USE
T1583.001	Acquire Infrastructure: Domain	JUDGMENT PANDA has purchased domains for use in targeted campaigns.
T1583.006	Acquire Infrastructure: Web Services	JUDGMENT PANDA has used GitHub to host malware linked in spearphishing e-mails.
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	JUDGMENT PANDA has created a Registry Run key named Dropbox Update Setup to establish persistence for a malicious Python binary.
T1059.003	Command and Scripting Interpreter: Windows Command Shell	JUDGMENT PANDA has used a tool to open a Windows Command Shell on a remote host.
T1059.006	Command and Scripting Interpreter: Python	JUDGMENT PANDA has used Python-based implants to interact with compromised hosts.
T1555.003	Credentials from Password Stores: Credentials from Web Browsers	JUDGMENT PANDA has used a tool to steal credentials from installed web browsers including Microsoft Internet Explorer and Google Chrome.
T1140	Deobfuscate/Decode Files or Information	JUDGMENT PANDA has used the AES256 algorithm with a SHA1 derived key to decrypt exploit code.
T1573.001	Encrypted Channel: Symmetric Cryptography	JUDGMENT PANDA has used AES encrypted communications in C2.
T1041	Exfiltration Over C2 Channel	JUDGMENT PANDA has exfiltrated files via the Dropbox API C2.
T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	JUDGMENT PANDA has exfiltrated stolen data to Dropbox.
T1068	Exploitation for Privilege Escalation	JUDGMENT PANDA has exploited CVE-2017-0005 for local privilege escalation.
T1105	Ingress Tool Transfer	JUDGMENT PANDA has used tools to download malicious files to compromised hosts.
T1036	Masquerading	JUDGMENT PANDA has spoofed legitimate applications in phishing lures and changed file extensions to conceal installation of malware.
T1036.004	Masquerade Task or Service	JUDGMENT PANDA has created a run key named Dropbox Update Setup to mask a persistence mechanism for a malicious binary.
T1027.002	Obfuscated Files or Information: Software Packing	JUDGMENT PANDA has used multi-stage packers for exploit code.

Continued on next page

TABLE 1: JUDGMENT PANDA TECHNIQUES (Continued)

T1566.002	Phishing: Spearphishing Link	JUDGMENT PANDA has used malicious links and web beacons in e-mails for malware download and to track hits to attacker-controlled URL's.
T1598	Phishing for Information	JUDGMENT PANDA targeted presidential campaign staffers with credential phishing e-mails.
T1012	Query Registry	JUDGMENT PANDA has used a tool to query the Registry for proxy settings.
T1218.007	System Binary Proxy Execution: Msiexec	JUDGMENT PANDA has used the msiexec.exe command-line utility to download and execute malicious MSI files.
T1082	System Information Discovery	JUDGMENT PANDA has used a tool to capture the processor architecture of a compromised host in order to register it with C2.
T1016	System Network Configuration Discovery	JUDGMENT PANDA has used a tool to enumerate proxy settings in the target environment.
T1033	System Owner/User Discovery	JUDGMENT PANDA has used a tool to capture the username on a compromised host in order to register it with C2.
T1124	System Time Discovery	JUDGMENT PANDA has used a tool to capture the time on a compromised host in order to register it with C2.
T1204.001	User Execution: Malicious Link	JUDGMENT PANDA has used malicious links in e-mails to lure victims into downloading malware.
T1102.002	Web Service: Bidirectional Communication	JUDGMENT PANDA has used Dropbox for C2 allowing upload and download of files as well as execution of arbitrary commands.

TABLE 2: SCARAB TECHNIQUES

T1566.001	Phishing: Spearfishing Attachment	Known campaign activity targeting Ukrainian governmental institutions using HeaderTip delivered via file attachment
T1204.002	User Execution: Malicious File	HeaderTip used in recent campaign activity by this actor in Ukraine required user execution.
T1059	Command and Scripting Interpreter	HeaderTip used in recent campaign activity by this actor in Ukraine was relying - also - on Windows Command Shell for execution.

Continued on next page

TABLE 2: SCARAB TECHNIQUES (Continued)

T1218.011	System Binary Proxy Execution: Rundll32	Actor has been known for executing malicious dlls from common folders with write permission.
T1112	Modify Registry	Actor has been known for using windows registry to store configuration files and for defense evasion.
T1547.001	Boot or Logon Autostart Execution:Registry Run Keys / Startup Folder	Actor has been known for modifying registry and startup folders to obtain persistence. Known registry entries for this use are 'httpshelper' and 'httpsrvlog'
T1102	Web Service	Actor has been known to use standard http methods for its C2. A domain 'product2020.mrbasic.com' and a user-agent 'Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko' have been confirmed for this use. Communication mostly used port 8080.

TABLE 3: MUSTANG PANDA TECHNIQUES

ID	NAME	USE
T1583.001	Acquire Infrastructure: Domain	MUSTANG PANDA have acquired C2 domains prior to operations.
T1071.001	Application Layer Protocol: Web Protocols	MUSTANG PANDA has communicated with its C2 via HTTP POST requests.
T1560.001	Archive Collected Data: Archive via Utility	MUSTANG PANDA has used RAR to create password-protected archives of collected documents prior to exfiltration.
T1560.003	Command and Scripting Interpreter: Windows Command Shell	MUSTANG PANDA has encrypted documents with RC4 prior to exfiltration.
T1119	Automated Collection	MUSTANG PANDA used custom batch scripts to collect files automatically from a targeted system.
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	MUSTANG PANDA has created the registry key HKEY_LOCAL_MACHINE\[...]\ AdobelmdyU to maintain persistence.
T1059.001	Command and Scripting Interpreter: PowerShell	MUSTANG PANDA has used malicious PowerShell scripts to enable execution.
T1059.003	Command and Scripting Interpreter: Windows Command Shell	MUSTANG PANDA has executed HTA files via cmd.exe, and used batch scripts for collection.
T1059.005	Command and Scripting Interpreter: Visual Basic	MUSTANG PANDA has embedded VBScript components in LNK files to download additional files and automate collection.

Continued on next page

TABLE 3: MUSTANG PANDA TECHNIQUES (Continued)

T1074.001	Data Staged: Local Data Staging	MUSTANG PANDA has stored collected credential files in c:\windows\temp prior to exfiltration. MUSTANG PANDA has also stored documents for exfiltration in a hidden folder on USB drives.
T1573.001	Encrypted Channel: Symmetric Cryptography	MUSTANG PANDA has encrypted C2 communications with RC4.
T1585.002	Establish Accounts: Email Accounts	MUSTANG PANDA has leveraged the legitimate email marketing service SMTP2Go for phishing campaigns.
T1546.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	MUSTANG PANDA's custom ORat tool uses a WMI event consumer to maintain persistence.
T1052.001	Exfiltration Over Physical Medium: Exfiltration over USB	MUSTANG PANDA has used a customized PlugX variant which could exfiltrate documents from air-gapped networks.
T1203	Exploitation for Client Execution	MUSTANG PANDA has exploited CVE-2017-0199 in Microsoft Word to execute code.
T1083	File and Directory Discovery	MUSTANG PANDA has searched the entire target system for DOC, DOCX, PPT, PPTX, XLS, XLSX, and PDF files.
T1564.001	Hide Artifacts: Hidden Files and Directories	MUSTANG PANDA's PlugX variant has created a hidden folder on USB drives named RECYCLE.BIN to store malicious executables and collected data.
T1574.002	Hijack Execution Flow: DLL Side-Loading	MUSTANG PANDA has used a legitimately signed executable to execute a malicious payload within a DLL file.
T1070	Indicator Removal: File Deletion	MUSTANG PANDA will delete their tools and files, and kill processes after their objectives are reached.
T1105	Ingress Tool Transfer	MUSTANG PANDA has downloaded additional executables following the initial infection stage.
T1036.005	Masquerading: Match Legitimate Name or Location	MUSTANG PANDA has used names like adobeupdate.dat and PotPlayerDB.dat to disguise PlugX, and a file named OneDrive.exe to load a Cobalt Strike payload.
T1036.007	Masquerading: Double File Extension	MUSTANG PANDA has used an additional filename extension to hide the true file type.
T1027	Obfuscated Files or Information	MUSTANG PANDA has delivered initial payloads hidden using archives and encoding measures.

Continued on next page

TABLE 3: MUSTANG PANDA TECHNIQUES (Continued)

T1027.001	Binary Padding	MUSTANG PANDA has used junk code within their DLL files to hinder analysis.
T1003.003	OS Credential Dumping: NTDS	MUSTANG PANDA has used vssadmin to create a volume shadow copy and retrieve the NTDS.dit file. MUSTANG PANDA has also used reg save on the SYSTEM file Registry location to help extract the NTDS.dit file.
T1566.001	Phishing: Spearphishing Attachment	MUSTANG PANDA has used spearphishing attachments to deliver initial access payloads.
T1566.002	Phishing: Spearphishing Link	MUSTANG PANDA has delivered web bugs and malicious links to their intended targets.
T1057	Process Discovery	MUSTANG PANDA has used tasklist /v to determine active process information.[8]
T1219	Remote Access Software	MUSTANG PANDA has installed TeamViewer on targeted systems.
T1091	Replication Through Removable Media	MUSTANG PANDA has used a customized PlugX variant which could spread through USB connections.[8]
T1053.005	Scheduled Task/Job: Scheduled Task	MUSTANG PANDA has created a scheduled task to execute additional malicious software, as well as maintain persistence.
T1518	Software Discovery	MUSTANG PANDA has searched the victim system for the InstallUtil.exe program and its version.[2]
T1608	Stage Capabilities	MUSTANG PANDA has used servers under their control to validate tracking pixels sent to phishing victims.
T1608.001	Upload Malware	MUSTANG PANDA has hosted malicious payloads on DropBox including PlugX.
T1218.004	System Binary Proxy Execution: InstallUtil	MUSTANG PANDA has used InstallUtil.exe to execute a malicious Beacon stager.
T1218.005	System Binary Proxy Execution: Mshta	MUSTANG PANDA has used mshta.exe to launch collection scripts.
T1082	System Information Discovery	MUSTANG PANDA has gathered system information using systeminfo.
T1016	System Network Configuration Discovery	MUSTANG PANDA has used ipconfig and arp to determine network configuration information.
T1049	System Network Connections Discovery	MUSTANG PANDA has used netstat -ano to determine network connection information.

Continued on next page

TABLE 3: MUSTANG PANDA TECHNIQUES (Continued)

T1204.001	User Execution: Malicious Link	MUSTANG PANDA has sent malicious links including links directing victims to a Google Drive folder.
T1204.002	User Execution: Malicious File	MUSTANG PANDA has sent malicious files requiring direct victim interaction to execute.
T1102	Web Service	MUSTANG PANDA has used Drop-Box URLs to deliver variants of PlugX.
T1047	Windows Management Instrumentation	MUSTANG PANDA has executed PowerShell scripts via WMI.