Divided we hack : exploring the degree of Sino-Russian coordination in cyberspace during the Ukraine war

Reference:
Ferazza Francesco, Melella Cosimo, Mersinas Konstantinos, Calcara Antonio.- Divided we hack : exploring the degree of Sino-Russian coordination in cyberspace during the Ukraine war
8th IEEE European Symposium on Security and Privacy (EuroS and P), JUL 03-07, 2023, TU Delft, ECHO, TU Delft, ECHO, Delft, Netherlands - ISSN 2768-0649 - Los alamitos, Ieee computer soc, (2023), p. 627-640
Full text (Publisher's DOI): https://doi.org/10.1109/EUROSPW59978.2023.00074
To cite this reference: https://hdl.handle.net/10067/1992350151162165141

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

Ferazza, Francesco; Melella, Cosimo; Mersinas, Konstantinos; Calcara, Antonio

Ieee computer soc, 2023. - ISBN 979-8-3503-2720-5 - 8th IEEE European Symposium on Security and Privacy (EuroS and P)

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 coordinate at the strategic level in the cyber domain, this article aims at better understanding whether these two nation-states also have their affiliated threat groups collaborating. 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 collaboration 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. Furthermore, we observe that a possible obstacle to coordination at the operational and tactical levels is the inherently complex and secretive nature of Advanced Persistent Threat (APT) activity: proper coordination would require sharing highly sensitive and critical information among the involved parties, such as details on the infrastructures, techniques, and procedures being used.

Keywords: *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[2] declared they detected hacks that had the attributes of the cyberwarfare unit of the People's Liberation Army.[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] or divergence[6] between the two NATO's strategic competitors and

[1] Maxim Tucker, "China accused of hacking Ukraine days before Russian invasion", *New York Times,* April 01, 2022; https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf

[2] SBU: Služba Bezpeky Ukrayiny (SBU)

[3] "Did China Help Moscow Hack Ukraine & Share Critical Intelligence Before The Russian Invasion?", *The EurAsian Times,* April 3, 2022; https://eurasiantimes.com/decoded-did-china-help-moscow-hack-ukraine-russian-invasion/ ; https://thehill.com/policy/cybersecurity/3256792-ukraine-intelligence-accuses-china-of-hacking-days-before-invasion-report/

[4] Gordon Corera, "Mystery of alleged Chinese hack on eve of Ukraine invasion", *BBC*, April 07, 2022, https://www.bbc.com/news/technology-60983346 ; Atsushi Teraoka, "Chinese hackers launch cyberattacks against Ukraine amid war", *Nikkei Asia*, April 07, 2022; https://asia.nikkei.com/Politics/Ukraine-war/Chinese-hackers-launch-cyberattacks-against-Ukraine-amid-war

[5] Perizat Risbek Kizi "China and Russia: between partnership and competition", *The Asia Today*, January 05, 2022. https://theasiatoday.org/editorials/china-and-russia-between-partnership-and-competition/; Paul Stronski, Nicole NG, "Cooperation and Competition: Russia and China in Central Asia, the Russian Far East, and the Arctic", *Carnegie Endowment for International Peace*, February 28, 2018; https://carnegieendowment.org/2018/02/28/cooperation-and-competition-russia-and-china-in-central-asia-russian-far-east-and-arctic-pub-75673

[6] Junuguru Srinivas, "Russia and China in BRICS: Convergences and Divergences" in *Future of the BRICS and the Role of Russia and China*. (Singapore: Palgrave Macmillan, 2022). https://doi.org/10.1007/978-981-19-1115-6_5

potential adversaries[7]. 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[8].

The research question we try to answer with this article is: "*While at a higher strategic level China and Russia are trying to coordinate in the cyber domain, do they also have their affiliated advanced threat groups coordinate and collaborate?*"
Hence, we explore whether the Chinese and Russian cyber-operations[9] were coordinated and, precisely, whether there are any links between the two countries' military-related Advanced Persistent Threat (APT) activities[10]. 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.".[11] Specialised investigations during the first ten months of the war showed that cyberattacks had a limited effect on the battlefield[12], but played an active role in gathering information and causing damage to Ukrainian critical infrastructure.[13] For instance, state-sponsored APTs (Advanced Persistent Threats)[14] have at times operated in

[7]Richard J. Harknett & Max Smeets Cyber campaigns and strategic outcomes, Journal of Strategic Studies, 2022 45:4, 534-567, DOI: 10.1080/01402390.2020.1732354

[8] Kello, Lucas, 'Cyber Disorders: Rivalry and Conflict in a Global Information Age', Presentation, International Security Program Seminar Series, Cambridge, Mass. International Security Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2012. http://www.belfercenter.org/publication/ cyber-disorders-rivalry-and-conflict-global-information-age

[9] Swaine, Michael D. "Chinese Views on Cybersecurity in Foreign Relations," China Leadership Monitor, October 7, 2013, http://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf.

[10] Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (New York: Oxford University Press, 2015)

[11] William Courtney, Peter A. Wilson, "If Russia Invaded Ukraine", *The RandBlog*, December 8, 2021; https://www.rand.org/blog/2021/12/expect-shock-and-awe-if-russia-invades-ukraine.html see also Jason Healey," Preparing for inevitable cyber surprise", *War on Rocks,* January 12, 2022; https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/ and Keir Giles," Putin does not need to invade Ukraine to get his way", *Chatman House,* December 21, 2021; https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way

[12] Jelena Vicic, Rupal N. Mehta, " Why Russian cyber dogs have mostly failed to bark", *War on Rocks,* March 14, 2022; https://warontherocks.com/2022/03/why-cyber-dogs-have-mostly-failed-to-bark/

[13] Digital Security Unit, "Special Report: Ukraine", *Microsoft*, April 27, 2022 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd; see also Maggie Miller, "Russian invasion of Ukraine could redefine cyber warfare", *Politico*, January 28, 2022; https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051; Carly Page, "US, UK and EU blame Russia for 'unacceptable' Viasat cyberattack", *TechCrunch*, May 10, 2022, https://techcrunch.com/2022/05/10/russia-viasat-cyberattack/
Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications", *Carnegie Endowment for International Peace*, December 16, 2022.
https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657

[14] According to National Institute of Standards and Technology (NIST) [3], an APT attacker: (i) pursues its objectives repeatedly over an extended period; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. See https://csrc.nist.gov/glossary/term/advanced_persistent_threat

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.[15]

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.[16] 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.[17] After all, the two countries have a long history of cooperation in cyberspace[18]. 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.[19] The two countries also worked together to promote the notion of "cyber sovereignty" in international organizations.[20] This created concerns about possible structured cooperation between the two countries in cyberspace.[21] 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

[15] Digital Security Unit, "Special Report: Ukraine", *Microsoft*, April 27, 2022 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd; see also Alex Scroxton," Russia-linked APTs targeted fleeing Ukrainian civilians", ComputerWeekly.com, July 21, 2022. https://www.computerweekly.com/news/252522996/Russia-linked-APT-targeted-fleeing-Ukrainian-civilians#:~:text=Two%20advanced%20persistent%20threat%20(APT,Mandiant%20and%20the%20US%20authorities; see also, Alex Scroxton, "Mandiant analysts: Russia-backed APTs likely to ramp up attack", January 21, 2022. https://www.computerweekly.com/news/252512299/Mandiant-analysts-Russia-backed-APTs-likely-to-ramp-up-attacks

[16] "Cyber Attacks from Chinese IPs on NATO Countries Surge by 116%", *Check Point,* March 21, 2022 https://blog.checkpoint.com/2022/03/21/cyber-attacks-from-chinese-ips-on-nato-countries-surge-by-116/

[17] Yuxi Wei, "China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty", *The Henry M. Jackson School of International Studies*, June 21, 2016 https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/

[18] Gilli, Andrea and Mauro Gilli, 'Why China Has Not Caught up Yet: MilitaryTechnological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage', International Security 43/3 (2019), 141–89. doi:10.1162/isec_a_00337.

[19] Government of the Russian Federation, "Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security", April 30, 2015. https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf.

[20] David Bandurski, "China and Russia are joining forces to spread disinformation", TechStream, March 11, 2022 https://www.brookings.edu/techstream/china-and-russia-are-joining-forces-to-spread-disinformation/

[21] Kelly Jackson Higgins, 'Chinese Cyberspies Pivot to Russia in Wake of Obama-Xi Pact', *DARKReading*, September 2, 2016, https://www.darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact/d/d-id/1324242. https://www.wsj.com/articles/BL-DGB-41673

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 Pand*a. 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.

One element that we believe is important to underline is that, in the context of cyberspace, we believe that cooperation and coordination are entirely different concepts. Coordination is another matter than cooperation, which 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, including those from Russia and China. However, the platform offers valuable insights. For example, by analysing 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[22] 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. While F3EAD is not specifically designed for APTs, the cycle principles can be adapted to illustrate the steps an advanced persistent threat might take during its operations. Here is a brief description of each cycle phase and how we applied it to study APTs and the degree - or lack - of coordination between them:
- *Find*: The Find stage involves identifying potential targets or sources of information. For this research it meant identifying known threat actors, and analysing publicly available information to identify potential vulnerabilities.
- *Fix*: The Fix step involves gathering more detailed information about the target. We used data, including network traffic analysis, to determine how the different APTs we analysed performed, harvesting information from human sources or open source information or using deception techniques to trick the APT into disclosing additional information.
- *Finish*: The Finish phase provides for the neutralisation of the target. For this research on APTs we evaluated the results of the collected data to determine whether the goals and objectives of the APTs had been met and matched our research goals. It involved evaluating the impact of the operations on the objectives considered, evaluating the accuracy and reliability of the information collected and identifying any opportunities for further research margins.

[22] Cooperation and coordination between different Advanced Persistent Threats (APTs) refer to the process by which these cyber threat actors or groups work together and synchronise their activities to achieve common goals in maximising the impact of their cyberattacks.

- *Exploit*: The Exploit phase involves collecting any information or material in the target site that may have intelligence value. In the context of this research on the cooperation between Russian and Chinese APTs, the Exploit phase was used to understand which payloads were used by the Chinese to gather information about their opponents' plans, also involving the exploitation of specific vulnerabilities in computer systems or networks to gain access to sensitive information.
- *Analysis*: The analysis phase involves analysing the information collected to identify patterns, connections and other valuable information for future operations. In the case of APTs, this could involve identifying the APT's motivations, tactics and objectives, and any weaknesses or vulnerabilities that could be exploited to disrupt or disrupt their operations.
- *Dissemination*: The dissemination phase involves sharing information with relevant staff and decision-makers. APTs could involve sharing information with other organisations, law enforcement or intelligence services to help build a more comprehensive understanding of the threat and develop effective countermeasures.

The lack of coordination between different APTs makes implementing the F3EAD intelligence cycle challenging. 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.

4. MUSTANG PANDA

Mustang Panda, also known as "RedDelta" or "Bronze President"[23], 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.[24] 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".[25] 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.[26] 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".[27] 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.[28] 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

[23] Names that have overlapping reference to a group entry and may refer to the same or similar group in threat intelligence reporting" - MITRE ATT&CK definition of associated groups, verbatim;

[24] Alexandre Côté Cyr, "Mustang Panda's Hodur: Old tricks, new Korplug variant", *ESET,* March 23, 2022; https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/

[25] Shane Huntley, "An update on the threat landscape", *Google Threat Analysis Group,* March 07, 2022; landscapehttps://blog.google/threat-analysis-group/update-threat-landscape-ukraine/

[26] Insikt Group, Chinese State-Sponsored Group 'Red Delta' targets the Vatican and Catholic organisations, Recorded Future, July 28, 2020. https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf

[27] Michael Raggi and Myrtus, "The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates", *Proofpoint*, March 07, 2022; https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european

[28] A PlugX version that could replicate via USB connections was also found, although its actual use has yet to be confirmed.

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.[29] 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 Благовещенск - Благовещенский Пограничный Оря.exe. The filename was chosen to target military officials and personnel familiar with the region. The Attack Chain in this specific attack would have started with the delivery of the executable "Blagoveshchensk - Blagoveshchensk Border Detachment [.] Exe", which appeared to be a legitimate document that used a PDF icon that, once opened, distributed the malware PlugX.[30]

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.[31] 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]."[32]

As of November 2022, there is little public and documented information available on Scarab[33]. 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

[29] Doug Bienstock, Melissa Derr, Josh Madeley, Tyler Mclellan, Chris Gardner, "UNC3524: Eye Spy on Your Email", *Mandiant,* November 1, 2022;
https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

[30] Kyaw Pyiyt Htet, Mitre Blog, https://attack.mitre.org/groups/G0129/

[31] Tom Hegel, "Chinese Threat Actor Scarab Targeting Ukraine", *SentinelLabs*, March 24, 2022;
https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/

[32] Atsushi Teraoka, "Chinese hackers launch cyberattacks against Ukraine amid war", *Nikkei Asia*, April 07, 2022;
https://asia.nikkei.com/Politics/Ukraine-war/Chinese-hackers-launch-cyberattacks-against-Ukraine-amid-war

[33] Yi Li, "Scarab attackers took aim at select Russian targets since 2012", *Broadcom,* January 22, 2015;
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8bfa7311-fdd9-4f8d-b813-1ab6c9d2c363&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

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[34].

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.[35]

6. JUDGMENT 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 "Judgment Panda".[36] 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.[37] 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.[38] 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.

[34] Common Vulnerability Exposure- CVE-2017-005, https://nvd.nist.gov/vuln/detail/CVE-2017-0005; https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0005

[35] Ravie Lakshmanan, "Another Chinese Hacking Group Spotted Targeting Ukraine Amid Russia Invasion", *The Hacker News,* March 26, 2022; https://thehackernews.com/2022/03/another-chinese-hacking-group-spotted.htmlAA

[36] Monica Kaminska, James Shires, and Max Smeets, " Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)", Tallinn Workshop Report, *ECCRI*, July, 22; https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf

[37] The group has also used vaccine-themed emails during the pandemic for their phishing efforts.

[38] Sergiu Gatlan, "Microsoft: State-backed hackers are targeting the 2020 US elections", BleepingComputer.com, September 10, 2020. https://www.bleepingcomputer.com/news/security/microsoft-state-backed-hackers-are-targeting-the-2020-us-elections/

There is evidence of them leveraging Dropbox APIs for their Communication and Control efforts.[39] 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.[40] 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. Conclusion

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[41]. 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[42]. Seldom have they been found using completely 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. Pro-Chinese groups have sensitive Russian information among their primary targets. We also highlight the difficulties in coordinating offensive cyber operations. Coordination in

[39] For instance, once the bot on the victim's system is registered with the attacker's server, it will check for new jobs by querying the Dropbox API endpoint: https://api[dot]dropboxapi.com/2/files/job. The bot can upload and download data to and from the endpoint and run tasks on the victim's machine via a simple python subprocess. Popen(...)

[40] Sumeet Wadhwani, "Russian Darknet Forum RAMP Reemerges With Chinese-speaking Hackers At the Wheel", *Spiceworks*, November 18, 2021.

[41] Bill Toulas, "Russian ransomware gangs start collaborating with Chinese hackers", BleepingComputer, November 17, 2021.

[42] Greg Austin, Kai Lin Tay, and Munish Sharma, "Great-Power Offensive Cyber Campaigns: Experiments in Strategy," International Institute for Strategic Studies, February 24, 2022, https://www.iiss.org/blogs/research-paper/2022/02/great-power-offensive-cyber-campaigns.

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.[43]

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.[44] 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[45] 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 also opens 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.[46] 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 helps scholars and analysts better grasp complex and multi-faceted phenomena such as APTs. Moreover, it helps public and international organisations like NATO or the EU and Western states better protect themselves against malicious cyber-activities.

[43] Winnona DeSombre and Dan Byrnes, “Thieves and Geeks: Russian and Chinese Hacking Communities”, *Recorded Future,* 2018. https://go.recordedfuture.com/hubfs/reports/cta-2018-1010.pdf

[44] Depending on the focus and resources of the operations, the C&C infrastructure could be like a single server operating on the external network or a whole series of operations to compromise legitimate web servers to use them for C&C subsequently.

[45] APTs work leveraging economies of scale. CYBER KILL CHAIN Whitepaper

[46] Max Smeets, Cyber Arms Transfer: Meaning, Limits, and Implications, *Security Studies*, 31:1, 65-91, 2022; DOI: 10.1080/09636412.2022.2041081