Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

The Strategic Role of Cyber Intelligence in Identifying Cyber Threats: An Empirical Study of Mustang Panda in South East Asia and Indonesia

Krisnayanto[1], Suryadi[2]

Abstract

The cyber espionage threat posed by the Mustang Panda group has become a critical concern in cybersecurity, particularly within the Southeast Asian region. This group targets strategic sectors in Indonesia, creating significant risks to national security. This study aims to examine the strategic role of intelligence in detecting and addressing these threats through an approach grounded in empirical data. By integrating data from cybersecurity reports and metadata analysis, the research identifies the operational patterns and modus operandi of the Mustang Panda group in Southeast metadata analysis and the operational patterns and modus operandi of the Mustang Panda group in Southeast Asia. Additionally, it addresses gaps in the existing literature, which predominantly focuses on technical aspects, by offering theoretical insights and practical contributions to developing both theoretical insights and practical contributions to the development of intelligence strategies. The findings reveal that a structured, evidence-based intelligence approach can significantly enhance the effectiveness of detecting and mitigating cyber espionage threats. Furthermore, the study provides a strategic framework to strengthen Indonesia's and South East Asia's Asia cyber intelligence capabilities and offers policy recommendations relevant to decision-makers. This research addresses a critical gap in the cybersecurity literature and makes a tangible contribution to managing increasingly complex cyber threats in the digital era.

Keywords: *Cyber Intelligence, Mustang Panda, Southeast Asia, Cyber espionage, Indonesia.*

Introduction

In the digital era characterized by global reliance on information and communication technology, the threat of cyber espionage has emerged as one of the most critical security challenges. Cyber espionage, the unauthorized collection of data or information via digital networks, has expanded rapidly alongside technological advancements. The targets of such activities are not limited to government and military entities but also extend to multinational corporations, academic institutions, and individuals. Technological innovations, including artificial intelligence (AI), the Internet of Things (IoT), and cloud computing, have broadened the scope of these threats. Sensitive information such as trade secrets, strategic state data, and personal records can serve as prime targets for perpetrators. These actors are not confined to state agencies; criminal groups and non-state organizations also play significant roles in this evolving threat landscape. The implications of cyber espionage are profound, affecting national security, economic stability, and individual privacy. High-profile incidents, such as the hacking of electoral systems, large-scale data breaches, and the infiltration of critical infrastructure like power grids or transportation networks, demonstrate the potential of these attacks to destabilize nations.

To address these threats, comprehensive mitigation strategies are essential. These should include strengthening cybersecurity policies, investing in advanced detection and prevention technologies, and raising public awareness about the importance of digital security. Furthermore, international collaboration is crucial in combating this global challenge, given its inherently transnational nature (Mansoor et al., 2020). In an increasingly connected digital age, the threat of cyber espionage has evolved into one of the biggest challenges to national security. Countries worldwide face significant risks from cyberattacks aimed at stealing sensitive information, damaging critical infrastructure, or disrupting political and economic stability (Banks, 2016). Indonesia, as a country with rapid economic growth and a strategic position in the Southeast Asian region, is becoming an increasingly attractive target for politically and economically motivated cyber

[1] School of Strategic and Global Studies, Universitas Indonesia, Indonesia, Email: krisnayanto01@ui.ac.id, krisnayantos3@gmail.com, https://orcid.org/0009-0006-0635-5701

[2] Professor, Faculty Mathematics and Natural Sciences, Universitas Indonesia, Indonesia, Email: suryadi.mt@sci.ui.ac.id, (Corresponding Author), https://orcid.org/0000-0002-3104-8520

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

actors (Lehmann, 2015). One group that has been of particular concern in this context is the Mustang Panda, a cyber entity that allegedly has affiliations with the interests of a specific country. Their activities in intensifying cyberattacks against important entities in Indonesia highlight the urgent need to understand and develop more effective detection strategies (Setiyawan, 2019). As a key component in a country's defense, intelligence plays a vital role in identifying, analyzing, and responding to these threats. However, the technical and tactical challenges in detecting sophisticated cyber operations, such as those conducted by the Mustang Panda, show that traditional intelligence approaches require significant adaptation and innovation to remain relevant and practical (Aulianisa & Indirwan, 2020).

Broader Context of Mustang Panda in Cyber Espionage

Mustang Panda is a well-documented cyber espionage group renowned for its sophisticated and persistent campaigns. Frequently linked to Chinese state-sponsored activities, the group primarily targets governmental, non-governmental, and private entities across various regions, including Southeast Asia, Europe, and the United States. Its operations exemplify broader trends in state-sponsored cyber activities, where advanced persistent threat (APT) groups are employed to achieve geopolitical, economic, and strategic objectives.

Key Characteristics and Modus Operandi

Mustang Panda is mainly known for employing spear-phishing campaigns and deploying custom malware, such as the PlugX remote access Trojan (RAT). These tools enable the group to infiltrate targeted systems, exfiltrate sensitive information, and maintain long-term access for sustained intelligence gathering. Their campaigns often exploit current geopolitical events to increase the effectiveness of phishing emails, reflecting a deep understanding of sociopolitical contexts.

Strategic Objectives and Implications

The activities of Mustang Panda align closely with China's broader strategic goals, which include maintaining regional dominance, securing economic interests, and achieving technological superiority. By targeting critical sectors such as government agencies, defense organizations, and research institutions, the group supports objectives like policy influence, counterintelligence, and gaining competitive advantages in emerging technologies.

Broader Trends in State-Sponsored Cyber Espionage

Mustang Panda's activities illustrate the increasing use of cyber espionage as a tool of statecraft in the digital era. Nation-states increasingly leverage cyber capabilities to achieve goals traditionally pursued through conventional espionage methods. This trend underscores the critical need for robust cybersecurity measures and international cooperation to counter these threats effectively.

Challenges in Attribution and Response

Attributing cyberattacks to specific actors, particularly state-sponsored groups, remains challenging due to the use of anonymization techniques and the global nature of the internet. Groups like Mustang Panda often operate within the gray zone of international law, complicating diplomatic and legal responses. This highlights the urgent need for stronger frameworks to address cyber espionage effectively at both national and international levels.

By examining the activities of Mustang Panda, stakeholders can gain valuable insights into the evolving landscape of cyber threats. Countering these challenges requires a combination of technical innovation, policy development, and global collaboration to build a more secure digital environment.

Mustang Panda is a prominent cyber espionage group often associated with Chinese state-sponsored activities. Known for its focus on Southeast Asia and other regions, the group primarily targets government

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

organizations, think tanks, NGOs, and industries involved in policy-making, research, and development. Here is a broader contextual analysis of the Mustang Panda operation in Southeast Asia (Hmaidi, 2023).

Table 1. Mustang Panda Operations Tactic, Tools, And Motivation

Active Since	Early 2010s. (Alaverronen & Pohjola, 2023)
Tactics	Primarily relies on spear-phishing and malware campaigns, leveraging tailored lures and socially engineered emails. (Mazurczyk & Caviglione, 2021)
Tools	Known for using PlugX malware and its derivatives, often disguised within seemingly legitimate files like PDF documents or compressed folders.(Mihelič et al., 2019)
Motivations	Intelligence gathering, focusing on political, economic, and strategic issues. (Bilgin, 2024)

Source: compiled by author, 2024.

Research Problem

Cyber threats to critical infrastructure continue to grow in scale and complexity, especially in the Southeast Asian region, which is at the center of geopolitical dynamics. In Indonesia, one of the significant threats comes from the Mustang Panda group, a cyber espionage entity that consistently targets strategic sectors, including the government, military, and technology industries. Despite the increasing prevalence of such threats, limited research comprehensively examines the specific tactics, techniques, and procedures (TTPs) employed by Mustang Panda in the Indonesian context. The lack of a robust national cybersecurity framework and limited public awareness about cyber risks also exacerbate Indonesia's vulnerability. This situation is further compounded by the challenges in attributing cyber attacks and the absence of regional cooperation mechanisms tailored to address state-sponsored cyber espionage. As a result, critical sectors remain exposed to potentially devastating disruptions and data breaches, threatening national security, economic stability, and technological sovereignty. Thus, The research problem centers on understanding the evolving threat landscape of Mustang Panda, identifying gaps in Indonesia's cyber defense capabilities, and exploring collaborative strategies to mitigate the risks of cyber espionage. Addressing this problem is essential for enhancing Indonesia's resilience against advanced persistent threats and ensuring the security of its critical infrastructure in an increasingly interconnected world. (Kurta, 2023).

Their activities include the collection of sensitive information and the exploitation of weaknesses in security systems, which can have a profound impact on national security. Nevertheless, traditional approaches to cyber threats are often inadequate to anticipate increasingly organized high-tech operations (Fokker, 2023). In addition, the intelligence strategy, which is supposed to be at the forefront of detecting this threat, is still not optimally integrated with the national security policy framework. This indicates an urgent need for research to develop effective and evidence-based intelligence strategies to detect and address cyber espionage threats, particularly from the Mustang Panda group (Duan et al., 2024).

Research Objectives

This study aims to analyze the strategic role of intelligence in detecting and dealing with cyber espionage threats, focusing on the Mustang Panda group's activities that target vital sectors in Southeast Asia and Indonesia. Through an empirical data-based approach, this study seeks to identify these groups' operational patterns, techniques, and strategies for launching their attacks. In addition, this research aims to develop a conceptual framework that can assist national security institutions in strengthening cyber intelligence capacity. By understanding threat patterns and exploring effective mitigation measures, this study is expected to provide relevant strategic recommendations for cybersecurity policymakers and practitioners facing similar future challenges. The results of this research contribute to developing cybersecurity literature and provide practical insights to improve Indonesia's national security resilience in increasingly complex cyber threats.

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

Outline of the Paper

This paper is organized as follows: The introduction provides an overview of cyber espionage threats and outlines the study's research problem, objectives, and structure. The Methodology details the qualitative research methods employed, including the analysis of secondary data sources. The Results section presents the findings from the comparative analysis of data related to the Mustang Panda Operation in Southeast Asia and Indonesia, emphasizing key actors and their interactions. The Discussion interprets these findings, focusing on the implications of the Mustang Panda Operation. Lastly, the Conclusion summarizes the main findings and their implications, offering policy recommendations and suggestions for future research. By examining the strategic role of intelligence in identifying cyber threats in Southeast Asia and Indonesia and exploring the strategies to combat cyber espionage, this study aims to contribute to a deeper understanding of how these interactions influence cybersecurity policy implementation and outcomes in Southeast Asian countries.

Methods

Research Design

This research adopts a qualitative approach grounded in empirical analysis to examine the strategic role of cyber intelligence in identifying cyber espionage threats posed by the Mustang Panda group in Southeast Asia and Indonesia. This research's secondary data is derived from publicly accessible and restricted sources.

Data Collection

Data on Mustang Panda's cyberattacks is gathered from cybersecurity reports published by leading organizations, such as Trend Micro, Palo Alto Networks, and GitHub. Additionally, reports from government agencies, scholarly journals, and news articles concerning Mustang Panda's activities in Southeast Asia and Indonesia are incorporated to enhance the depth of the metadata analysis techniques employed to investigate attack patterns, domain usage, and infiltration strategies frequently employed by Mustang Panda. This analysis is based on data available online.

Data Analysis

The data that has been collected is analyzed using a thematic analysis approach to identify attack patterns, modus operandi, and the main targets of the Mustang Panda group in Southeast Asia, including Indonesia. The analysis also focused on the interaction between the Mustang Panda group's attack methods and the existing intelligence response. Analytical Framework: The research uses a conceptual framework based on cybersecurity theory and strategic intelligence to connect empirical data with threat mitigation strategies. Data Triangulation: Triangulation techniques are used to ensure data validity by comparing information from various sources, including incident reports and public data. This study uses a case study approach to delve deeply into the activities of Mustang Panda in Indonesia. This case study analyzes documented cyber espionage incidents, including their timing, methods, and impact on national security.

Ethical Considerations

This research adheres to ethical principles in data collection and analysis. To maintain informants' confidentiality and avoid law or privacy violations, sensitive information is treated carefully.

Result and Discussion

Research result

Southeast Asia is a geopolitically significant region, making it a high-priority target for China's cyber espionage. Mustang Panda, also known as Earth Preta or Bronze President, is a China-based advanced

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

persistent threat (APT) group active since at least 2012. The group is well-known for its cyber espionage campaigns, particularly those targeting Southeast Asian government entities with strategic targets as follows:

Table 2. Mustang Panda's Strategic Target

Geopolitical Importance	The region sits at the crossroads of major trade routes, including the South China Sea. ASEAN (Association of Southeast Asian Nations) plays a key role in regional stability and economic growth. Territorial disputes, especially over the South China Sea, heighten China's interest in monitoring Southeast Asian states. (Commission et al., 2014)
Strategic Goals:	Collecting intelligence on regional alliances, military capabilities, and political strategies. Monitoring ASEAN negotiations and the involvement of external powers like the United States, Japan, and India. Gaining insights into trade agreements and economic collaborations. (Ball, 2011)
Targets:	Government Agencies: Ministries of foreign affairs, defense, and trade. NGOs and Think Tanks: Human rights advocacy or policy research entities. Critical Infrastructure: Energy, telecommunications, and maritime sectors. (Rehmat, n.d.)
Broader Implications	National Security Threat: Cyber-espionage undermines the sovereignty of affected states by exposing sensitive political, military, and economic information. Information stolen can be used to influence decision-making or gain leverage in negotiations. Regional Instability: Uneven cybersecurity capabilities across ASEAN nations create vulnerabilities that adversaries can exploit. Persistent cyber threats can erode trust among nations, especially when linked to state-sponsored actors. (Mahadevan, 2019a)
Economic Impact	Theft of intellectual property and trade secrets can hinder regional economic growth. Businesses in emerging markets face significant costs to enhance cybersecurity defenses. (Fokker, 2023)
Influence on Cyber Policy	Mustang Panda's activities highlight the need for stronger regional cooperation in cybersecurity. (Wang, 2024)

Source: compiled by author, 2024

Table 3. Modus Operandi of Mustang Panda

	Southeast Asia	Indonesia
Attack Patterns and Infiltration Techniques	Spear-Phishing Campaigns: Mustang Panda frequently employs spear-phishing emails containing malicious attachments or links to compromise their targets. For example, in June 2024, the group conducted a campaign using emails with .url attachments that deployed a signed downloader known as DOWNBAIT. This campaign targeted countries such as Myanmar, the Philippines, Vietnam, Singapore,	

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

	Cambodia, and Taiwan. The filenames and decoy documents were specifically tailored to align with the interests of these regions. (Trinh, 2024)	
Exploitation of Legitimate Software	The group has also been observed weaponizing legitimate software to facilitate their attacks. They exploited Visual Studio Code's embedded reverse shell feature to execute arbitrary code and deliver additional payloads. They established a reverse shell connection to the target's machine by issuing specific commands, enabling extensive control over the compromised system. (Rehmat, n.d.)	
DLL Side-Loading:	Mustang Panda uses DLL side-loading techniques to execute malicious code. In August 2023, the group targeted a government entity in the Philippines by delivering a malicious ZIP archive containing a rogue dynamic-link library (DLL). This method allowed the DLL to communicate with a remote server, granting unauthorized access to the system. (Mahadevan, 2019b)	
Custom Malware Deployment:		The group employs custom malware such as PUBLOAD, a downloader designed to facilitate the delivery of the PlugX malware. PUBLOAD conducts reconnaissance on infected networks and collects sensitive files, including documents and spreadsheets. Additionally, it acts as a gateway for supplementary tools like FDMTP, a secondary control tool, and PTSOCKET, an alternative method for data exfiltration. (Rahim et al., 2023)
Data Exfiltration Techniques	Exfiltrated data is typically compressed into an RAR archive and transferred to an attacker-controlled FTP site using cURL. Mustang Panda also utilizes the custom PTSOCKET program for multi-threaded file transfers, significantly enhancing their data exfiltration capabilities. (Mahadevan, 2019a)	

Source: compiled by author, 2024.

Metadata analysis involves the study of data that provides information about other data, such as file attributes, email headers, and network traffic details. In the context of Mustang Panda's activities, metadata

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

analysis can uncover patterns that indicate their involvement (Dorais-Joncas & Munõz, 2021). For example, during spear-phishing campaigns, the group often employs specific file naming conventions and document properties tailored to their target region. Filenames and decoy documents were customized for countries such as Myanmar, the Philippines, Indonesia, and Vietnam (Mahadevan, 2020). By analyzing the metadata of these documents, such as author names, creation times, and embedded language settings, it is possible to identify and attribute the malicious activity to Mustang Panda.

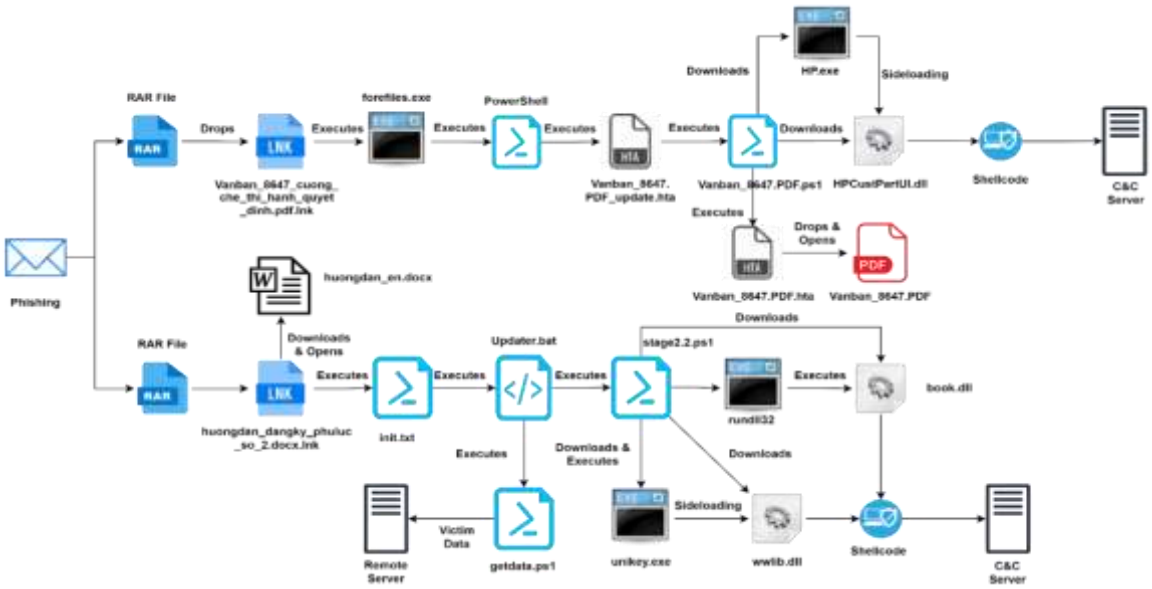

Figure 1. Overview of Mustang Panda Campaign in Vietnam (©Trend Micro 2024).

Between 2019 and 2024, reports from Indonesian government agencies indicate a significant increase in activities by Mustang Panda, targeting critical infrastructure and political institutions within the country. These reports highlight the group's strong interest in Indonesia's strategic resources and political landscape. Evidence suggests that this group may have targeted and compromised Indonesia's intelligence agency, Badan Intelijen Negara (BIN) (Panda, n.d.). This analysis explores the tactics, techniques, and procedures (TTPs) utilized by Mustang Panda, the potential implications of such breaches, and recommendations for future mitigation strategies. Additionally, multiple sources have reported Mustang Panda's attempts to infiltrate electoral systems during Indonesia's recent elections. These efforts seem to have been directed toward gaining insights into political strategies and potentially influencing electoral outcomes (Kurta, 2023).

Mustang Panda threat in the Indonesia context

Research on cyber espionage threats conducted by the Mustang Panda group against Indonesia revealed several significant findings reflecting their activities' complexity and scope. Here are the main results of this study:

Vulnerability of Indonesia's Cyber System

National policy limitations represent a significant factor contributing to Indonesia's vulnerability to cyber espionage. The absence of comprehensive, enforceable, and adaptive cybersecurity policies creates systemic weaknesses, leaving critical sectors exposed to advanced persistent threats (APTs) such as those posed by groups like Mustang Panda. The lack of cybersecurity infrastructure in Indonesia significantly heightens the risk of cyber espionage, particularly from advanced groups like Mustang Panda. Addressing these gaps requires a holistic approach that combines technological, policy, and human resource development efforts. Low public awareness of cybersecurity poses a critical risk to Indonesia's resilience against cyber espionage. Addressing this challenge requires a multi-faceted approach involving education, training, and widespread public engagement. National policy limitations significantly weaken Indonesia's ability to defend against

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

cyber espionage threats. Addressing these gaps requires comprehensive legislation, robust enforcement, proactive threat intelligence, and strengthened collaboration at both domestic and international levels.

Potential Impact

The cyber espionage activities of Mustang Panda have had far-reaching consequences for Indonesia, particularly in the areas of sensitive information leaks, operational disruptions, and threats to national sovereignty. Threats from the Mustang Panda have severe impacts. Mustang Panda's cyber espionage operations in Indonesia pose serious risks by leaking sensitive information, disrupting critical operations, and threatening national sovereignty. Addressing these impacts requires a cohesive effort at national and international levels to build robust defenses and mitigate vulnerabilities.

Mitigation Strategies

This study suggests several mitigation measures to address counter Mustang Panda's sophisticated cyber espionage campaigns in Indonesia, a comprehensive mitigation strategy is necessary. This strategy should encompass policy reforms, technological advancements, capacity-building initiatives, and international cooperation. Mitigating the impact of Mustang Panda's cyber espionage activities in Indonesia requires a holistic approach that combines policy development, technological investment, capacity building, and international collaboration.

Discussion

The analysis highlights that Mustang Panda's operations are closely tied to geopolitical goals, with a clear intention to destabilize the region and gather strategic intelligence. Their activities in Indonesia and Southeast Asia emphasize the urgent need for stronger cybersecurity measures and greater regional cooperation to reduce the group's influence.

Here are the recommendations

- Strengthen Cybersecurity Measures: Governments and organizations in Southeast Asia should prioritize modernizing their systems and adopting multi-layered security protocols to defend against Mustang Panda's tactics.

- Enhance Intelligence Sharing: Closer collaboration among ASEAN members and international cybersecurity firms can improve the early detection and swift response to Mustang Panda's campaigns.

- Promote Public Awareness: Launching education campaigns for the public and employees about phishing schemes and safe online practices can help lower the success rate of Mustang Panda's social engineering strategies.

- Develop Policies and Legislation: Regional governments should consider implementing stricter cybersecurity laws and allocating resources to build more substantial infrastructure for countering advanced threats.

Future Research Directions

Rigorous, systematic, and multidisciplinary academic research on Mustang Panda's cyber espionage activities holds significant potential to advance the field of cybersecurity. Future studies should address key gaps in understanding the group's operations, impact, and countermeasures. Below are suggested research directions that could contribute to a more comprehensive understanding of Mustang Panda and state-sponsored cyber espionage:

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

Socio-Political Factors Shaping Targeting Strategies

Understanding the socio-political context driving Mustang Panda's activities is essential for predicting future threats. Research in this area could include:

- Geopolitical Influence: Assessing how regional tensions and global power dynamics shape the group's focus on specific countries or sectors, particularly Southeast Asia.
- Economic Motivations: Exploring whether economic competition or industrial espionage plays a significant role in the selection of targets.
- Cultural and Historical Analysis: Investigating how historical ties or disputes influence the group's targeting decisions.

Evaluation of Existing Cyber Defense Mechanisms

Another important area is the assessment of current defensive measures against Mustang Panda's tactics, techniques, and procedures (TTPs). Research could explore:

- Effectiveness of Cybersecurity Tools: Evaluating the performance of existing threat detection and prevention tools in identifying and mitigating Mustang Panda's activities.
- Incident Response Frameworks: Analyzing how well national and organizational response frameworks address incidents involving this group.
- Policy and Regulation Impact: Reviewing the role of international and national cybersecurity policies in reducing vulnerabilities to state-sponsored cyber espionage.

Application of Advanced Threat Intelligence Tools

Future research should incorporate advanced technologies to enhance the analysis of Mustang Panda's activities. These could include:

- Machine Learning and AI: Leveraging artificial intelligence to predict attack patterns and identify real-time anomalies in real time.
- Big Data Analytics: Using large-scale data analysis to detect trends and correlations in Mustang Panda's operations.
- Blockchain for Attribution: Exploring blockchain technologies to improve transparency and attribution in cyber espionage incidents.

Cross-Disciplinary Research Collaboration

Given the multifaceted nature of cyber espionage, collaboration across disciplines—such as computer science, political science, sociology, and law—could provide richer insights. This could include:

- Legal and Ethical Implications: Investigating the legal challenges in addressing state-sponsored cyber espionage and proposing frameworks for international cooperation.
- Human Factors in Cybersecurity: Examining the role of human behavior and organizational culture in mitigating risks associated with spear-phishing and social engineering.

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

Regional and International Cooperation

Finally, research should emphasize the importance of collaboration within Southeast Asia and beyond to develop a unified response to Mustang Panda and similar threats. Key areas include:

- Regional Security Frameworks: Studying the effectiveness of ASEAN-led initiatives in addressing cyber threats.
- Information Sharing Mechanisms: Proposing models for improved information sharing among countries to enhance threat intelligence.
- Capacity Building: Exploring strategies for strengthening the cybersecurity capabilities of countries with limited resources.

Conclusion

Data analysis from reputable sources highlights Mustang Panda's persistent and evolving threat to Southeast Asia, particularly Indonesia. This research confirms that Mustang Panda is a real threat to cybersecurity in Indonesia, especially to strategic sectors. Therefore, a proactive and coordinated response is essential to improve national cyber resilience in the face of advanced threats. Their campaigns demonstrate high sophistication and align closely with geopolitical objectives. Strengthening regional cooperation in cybersecurity and implementing advanced threat detection systems are critical steps to mitigating the risks posed by such groups. The Mustang Panda advanced persistent threat (APT) group continues to exploit vulnerabilities in Southeast Asia, leveraging them for geopolitical advantage. By synthesizing data from leading cybersecurity firms, government reports, and academic research, this analysis offers actionable insights to counter the group's operations. Sustained vigilance and coordinated efforts are essential to protect the region from these sophisticated threats. The strategic role of intelligence in combating cyber espionage lies in its capacity to proactively identify, analyze, and neutralize threats. This involves real-time threat intelligence gathering, profiling adversaries, early attack detection, and leveraging counterintelligence measures to disrupt malicious activities. Collaborative initiatives, including partnerships with public and private organizations and insider threat monitoring, further bolster defense capabilities. Intelligence enhances supply chain security, advocates for stronger cybersecurity policies, and ensures resilience through robust response mechanisms. Continuous education and integration of advanced technologies, such as artificial intelligence (AI), significantly strengthen these strategies. Intelligence is the foundation of effective cyber espionage defense by offering foresight, actionable insights, and a framework for proactive and reactive measures. Organizations can develop a resilient posture by incorporating intelligence into all facets of cybersecurity, from threat detection to policy advocacy. This approach defends against existing threats and anticipates and adapts to evolving adversarial tactics. The key lies in adopting a holistic strategy integrating technological innovation, strategic collaboration, and human expertise.

References

Alaverronen, S., & Pohjola, J. (2023). Pandas in action: analysis of China related advanced persistent threat actors' tactics, techniques &procedures. jyx.jyu.fi. https://jyx.jyu.fi/handle/123456789/90108

Aulianisa, S. S., & Indirwan, I. (2020). Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia. Lex Scientia Law Review. https://journal.unnes.ac.id/sju/index.php/lslr/article/view/38197

Ball, D. (2011). China's cyber warfare capabilities. Security Challenges. https://www.jstor.org/stable/26461991

Banks, W. C. (2016). Cyber espionage and electronic surveillance: Beyond the media coverage. Emory LJ. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/emlj66&section=19

Bilgin, A. (2024). A New and Complicated Threat to European Security: China. Ulisa: Uluslararası Çalışmalar Dergisi. https://dergipark.org.tr/en/pub/ulisa/issue/85839/1484047

Commission, C. M., Congress, W. C., Firewall, G., Jinping, P. X., Strategy, M., Us, T., States, U., & Party, D. P. (2014). 4 . China ' s Cyber Influencing and Interference. 72–98.

Dorais-Joncas, A., & Munõz, F. (2021). Jumping the air gap. web-assets.esetstatic.com. https://web-assets.esetstatic.com/wls/2021/12/eset_jumping_the_air_gap_wp.pdf?ref=upstract.com&curator=upstract.com&utm_source=upstract.com

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 1064 – 1074
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5912

Duan, J., Luo, Y., Zhang, Z., & Peng, J. (2024). A heterogeneous graph-based approach for cyber threat attribution using threat intelligence. Proceedings of the 2024 16th …. https://doi.org/10.1145/3651671.3651707

Fokker, J. (2023). The CyberThreat report unveils financial, telecom, and energy sectors increasingly under attack. MoneyMarketing. https://doi.org/10.10520/ejc-nm_monm_v2023_n7_a21

Hmaidi, A. (2023). "HERE TO STAY"–CHINESE STATE-AFFILIATED HACKING FOR STRATEGIC GOALS. tnchtr4676.merics.org. https://tnchtr4676.merics.org/sites/default/files/2023-11/MERICS Report medium_Hacking.pdf

Kurta, N. C. L. (2023). Cyber Security Stagnation in Indonesia and the Philippines: a Comparative Case Study of their Strategies. dspace.cuni.cz. https://dspace.cuni.cz/handle/20.500.11956/187342

Lehmann, M. (2015). The case for an offensive ADF cyber capability: Beyond the Maginot mentality. Australian Defence Force Journal. https://search.informit.org/doi/abs/10.3316/informit.710796085002286

Mahadevan, P. (2019a). Cybercrime. In Threats during the COVID. globalinitiative.net. https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf

Mahadevan, P. (2019b). Cybercrime. In Threats during the COVID. globalinitiative.net. https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf

Mahadevan, P. (2020). Threats during the COVID-19 pandemic. April.

Mazurczyk, W., & Caviglione, L. (2021). Cyber reconnaissance techniques. Communications of the ACM, 64(3), 86–95. https://doi.org/10.1145/3418293

Mansoor, M., Fatima, T., & Ahmad, S. (2020). Signaling effect of brand credibility between fairness (price, product) and attitude of women buyers. Abasyn University Journal of Social Sciences, 13(1), 263.

Mihelič, A., Jevšček, M., Vrhovec, S., & Bernik, I. (2019). Testing the human backdoor: organizational response to a phishing campaign. Journal of Universal Computer Science, 25(11), 1458–1477. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85076928832&partnerID=40&md5=90ae317e483ac5e7aa52de782842d7b2

Panda, M. (n.d.). Indonesia denies report of Chinese hacking group breaching intelligence agency servers.

Rahim, A. S., Widodo, P., Reksoprodjo, A. H. S., & … (2023). Identify Cyber Intelligence Threats in Indonesia. International Journal Of …. http://ijhess.com/index.php/ijhess/article/view/426

Rehmat, S. (n.d.). Hybrid Warfare : Cyber Espionage , Economic Coercion , and Information Campaigns in the US-China Rivalry.

Setiyawan, A. (2019). NATIONAL CYBERSECURITY POLICY IN THE US AND INDONESIA. UNTAG Law Review. http://jurnal.untagsmg.ac.id/index.php/ulrev/article/view/1071

Trinh, V. D. (2024). Vietnam's Securitisation of Cybersecurity Under the Influence of a Rising China. Australian Journal of International Affairs. https://doi.org/10.1080/10357718.2024.2431039

Wang, W. (2024). Innovative strategies and forward thinking on China's digital maritime law enforcement. Marine Policy, 169, 106369. https://doi.org/https://doi.org/10.1016/j.marpol.2024.106369.