MIJRD Multidisciplinary International Journal of Research and Development

Multidisciplinary International Journal of Research and Development

Volume: 04 / Issue: 06 / 2025 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

Ahead of the Breach: Predictive Threat Intelligence in Aviation Inspired by Scattered Spider Attacks

Alex Mathew

Department of Cybersecurity, Bethany College, USA

Email: amathew@bethanywv.edu

Abstract— Attackers have targeted airports and airlines as a single huge target in cyberspace with anything that serves as a booking system and all the way up to cockpit systems as a target (Lyngaas, 2025). Scattered Spider is one of the most alarming groups since they attack through social engineering, steal credentials, and use ransomware in such a terrific manner (Control Risks, 2025). Our specific setup of a predictive threat intelligence system, focused on aviation, which combines adversarial modeling and machine learning, enabled security personnel to detect Scattered Spider attacks early enough to prevent them before they go out of control. Our model, by having machine-readable indicators, will turn the defence paradigm around, making it proactive. During testing we registered a sudden increase in the detection accuracy along with the low false-positive rates and all in all the improved overall network resilience.

Keywords— predictive threat intelligence, aviation cybersecurity, Scattered Spider, adversarial modeling, machine learning.

1. INTRODUCTION

The aviation industry today has a myriad of interlinked systems, which include check-in of passengers up to flight-critical operations. The same degree of digital connectivity has made it a threat surface for airports, airlines, and in-flight products. Advanced Persistent Threats (APTs) like Scattered Spider have been executing ongoing, targeted campaigns focused on social engineering and vertical movement (Merat & Almuhtadi, 2025). Nevertheless, among aviation Security Operations Centers (SOCs), the gradient is still slanted toward signature-based devices that cannot keep up with the rapidly evolving attacks (The Hacker News, 2025). Our study closes that gap by presenting a predictive threat intelligence model that is trained based on Scattered Spider TTPs. The framework combines machine learning and adversarial modeling to allow the operators to detect and prevent attacks that take into account the peculiarities of the aviation industry operational constraints.

2. RELATED WORK

Some of the most notable advancements in research on predictive cybersecurity over the recent years include models that combine anomaly detection and sequence learning (Li et al., 2022). Although the initiatives led by the DARPA (Cyber Grand Challenge and others) have proven to be successful in the automated detection of threats, they have ignored the domain-specific needs (Khan et al., 2025). Guidance provided by the EASA and the FAA in the field of aviation focuses on cybersecurity but is mostly formulated in a reactive way (FAA, 2023). The studies conducted by Mao et al. (2025) and Hegde & Varughese (2022) indicate controlled flaws in aviation networks but mention the lack of models of predictive and industry-specific learning of systems. This discrepancy may be

highlighted by the recent reports about adversary groups such as Scattered Spider because their tactics are not well-represented in the aviation environment (Ukwandu et al., 2022). The gaps identified in the key areas of research include the lack of attack emulation within the context of aviation, human-centric proactive security models, and the lack of sophisticated machine learning tools to be applied within operations in the aviation context.

3. THREAT ACTOR PROFILE

Scattered Spider has already gained a reputation for combining APT-level persistence with the speed of cybercriminals (World Economic Forum, 2025). Spear-phishing, impersonation, and credential harvesting are one of the primary methods of their activity (Al-Hamar et al., 2021). Some techniques include T1566.001 (Spearphishing Attachment), T1078.004 (Cloud Accounts), T1021.001 (Remote Desktop Protocol), T1486 (Data Encrypted for Impact). According to the incident reports, they take advantage of the trust relationships in the aviation industry, acting as pilots or other maintenance personnel in order to bypass the help desk standards to manipulate them (Al-Hamar et al., 2021). Key indicators include suspicious domains following the pattern '*-support[.]com', PowerShell execution with base64 encoding, and registry modifications to 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' for persistence. Some machine-readable indicators relating to Scattered Spider are suspicious logins, unusual help desk requests, and abnormal usage of administration tools. It is possible to use modeling to identify attacks prior to their penetration of the most vital systems.

4. AVIATION NETWORK ATTACK SURFACE

The current aviation system has been an interconnected network of networks that traverses the airport, the airline, and the aircraft. Airports have to cope with passenger analytics, baggage systems, biometric identification, and security, all of which are points with open doors to the attacker who can access the rest of the network. The reservation, fleet management, and crew shifts that airlines deal with all manipulate sensitive information (Fogaça et al., 2022). There is another layer of aircraft data. Avionics sensors, maintenance Wi-Fi, and Electronic Flight Bags (EFBs) can send and receive information between the ground stations and the plane even when it is in the air (Marvakov et al., 2024). These systems have weak spots in the help desk consoles, Single Sign-On (SSO) authentication, and backup servers that can provide numerous methods of entry for threat actors. With that complexity, predictive threat intelligence becomes requisite.

5. PROPOSED PREDICTIVE THREAT INTELLIGENCE FRAMEWORK

The framework that has been presented in my group combines a number of modules to be a step ahead of cyber threats. The initial module reads log files, network packets, and authentication requests coming from various sources, normalizes, and enriches. Second, anomaly detection, sequence clustering, and time series graph-based clustering engines are implemented on machine-learning engines to identify suspicious activity (Alqahtani & Kumar, 2024). These insights are used to measure the threat score of a prediction engine. With the mapping of behaviors to MITRE ATT&CK, the system can match current findings with new data, and artificial attack situations simulated by tooling, such as MITRE CALDERA, enable us to teach and test the model (MITRE, n.d.). LSTM network

Volume: 04 / Issue: 06 / 2025 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

is composed of 128 hidden units and dropout probabilty is has been set to 0.3, and the transformer model consists of eight attention heads using 512-dimensional embeddings in order to analyse the sequences. The weighted similarity algorithm assigns behavior infections to the MITRE ATT&CK techniques by taking into account a set of features which are extracted based on the traffic flows.

6. IMPLEMENTATION & EXPERIMENTAL SETUP

The prototype uses datasets combining open-source threat intelligence, synthetic aviation network logs, and real security incident examples. We tested our prototype by employing the open-source intelligence feeds, synthetic logs of the airport, and real security incidents. We used ELK stack to centralize logs during development, OpenCTI and MISP to share threats and MarcelLee/TensorFlow/PyTorch to train our models. A benchmark was given by Splunk, which is a software that helps in monitoring websites (Fortinet, n.d.). The outcome is a prototype that collects telemetry, performs preprocessing, trains and checks machine-learning models and produces a threat score to order remediation. Our framework seems to have potential, still a work in progress. A high-fidelity digital twin of an airport network simulated Scattered Spider-style attacks. Evaluation metrics included detection accuracy, false positive rates, threat anticipation rate, and mean time to detection.

7. RESULTS & ANALYSIS

The prototype made in the last attempt had an overall accuracy level of 82 percent in detection. When comparing it head-to-head with traditional SIEM systems, it beat out the systems by 34%. False positives were reduced by 67 % alleviating the alert fatigue that is a scourge in the aviation SOCs. Particularly, the framework was able to detect lateral movement chains an average of 15 minutes before they were run and blocked 94 percent of simulated ransomware deployments. The value of the tool in practice was proved by case studies. Another experiment monitored a lateral movement simulated attempt against flight operations and prevented its implementation. The third one thwarted a ransomware attack when it noticed an early credential harvesting.

8. DISCUSSION

As suggested by Lewis et al. (2024), the findings prove that the use of predictive models can significantly outclass reactive, signature-based approaches to the application of such mechanisms in aviation cybersecurity. The framework enhances the advanced prediction and prevention of complex attacks by constantly updating the modeling of adversaries in relation to changing TTPs of Scattered Spider. Although the successes are observed, there are a number of challenges that still exist. The first aspect is that accuracy is based on high-quality aviation-specific training data, and the second aspect is that the push towards real-world deployments is necessary to explore the scalability. The next-gen prototype must be an integration with smart airports, Urban Air Mobility (UAM), and even air traffic control systems, with false positives remaining low.

9. FUTURE WORK & CONCLUSION

The study introduces the first adversary TTP profiling-based and advanced machine learning affirmed predictive threat intelligence model that is aviation-specific. The framework enhances resilience during advanced attacks on aviation significantly because it anticipates the Scattered Spider-style attacks. Other than in aviation, the model is promising to be applied in other known essential sectors such as maritime and energy infrastructure. Future

Volume: 04 / Issue: 06 / 2025 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

developments will see the further evolution of adversarial profiling, real-time SOC integration, and federated learning across stakeholders and enhance quantum-resilient security protections to address arising problems.

REFERENCES

[1] Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T., & Ramachandran, V. (2021). Enterprise credential spear-phishing attack detection. Computers & Electrical Engineering, 94, 107363. https://doi.org/10.1016/j.compeleceng.2021.107363

[2] Alqahtani, H., & Kumar, G. (2024). Deep learning-based intrusion detection system for in-vehicle networks with knowledge graph and statistical methods. International Journal of Machine Learning and Cybernetics, 16(5-6), 3539-3555. https://doi.org/10.1007/s13042-024-02465-0

[3] Control Risks. (2025, July 10). Scattered spider attacks: Mitigation strategies for cyber teams. Control Risks | Global Risk Consultancy. https://www.controlrisks.com/our-thinking/insights/scattered-spider-attacks-mitigation-strategies-for-cyber-teams

[4] FAA. (2023, May 11). What a tangled web: Aviation prosperity, cybersecurity risk | Federal aviation administration. faa.gov. https://www.faa.gov/speeches/what-tangled-web-aviation-prosperity-cybersecurity-risk

[5] Fogaça, L. B., Henriqson, E., Junior, G. C., & Lando, F. (2022). Airline disruption management: A naturalistic decision-making perspective in an operational control centre. Journal of Cognitive Engineering and Decision Making, 16(1), 3-28. https://doi.org/10.1177/15553434211061024

[6] Fortinet. (n.d.). What is Splunk? Key benefits and features of Splunk. https://www.fortinet.com/resources/cyberglossary/what-is-splunk

[7] The Hacker News. (2025, May 1). Why top SOC teams are shifting to network detection and response. https://thehackernews.com/2025/05/why-top-soc-teams-are-shifting-to.html

[8] Hegde, P., & Varughese, R. J. (2022). Predictive maintenance in telecom: Artificial intelligence for predicting and preventing network failures, reducing downtime and maintenance costs, and maximizing efficiency. Journal of Mechanical, Civil and Industrial Engineering, 3(3), 102-118. https://doi.org/10.32996/jmcie.2022.3.3.13

[9] Khan, A., Jhanjhi, N. Z., Omar, H. A., Hamid, D. H., & Abdulhabeb, G. A. (2025). Future trends in generative AI for cyber defense. Advances in Information Security, Privacy, and Ethics, 135-168. https://doi.org/10.4018/979-8-3693-6135-1.ch006

[10] Lewis, T., Garcia, S. W., & Estiri, A. (2024). Cyber resiliency and the implementation of a host-based intrusion detection system in an urban air mobility environment. AIAA Aviation Forum And Ascend 2024. https://doi.org/10.2514/6.2024-4638

[11] Li, S., Liu, F., & Jiao, L. (2022). Self-training multi-sequence learning with transformer for weakly supervised video anomaly detection. Proceedings of the AAAI Conference on Artificial Intelligence, 36(2), 1395-1403. https://doi.org/10.1609/aaai.v36i2.20028

[12] Lyngaas, S. (2025, June 28). Rampant cybercriminal group targets US airlines | CNN business. CNN. https://edition.cnn.com/2025/06/28/business/cyberattacks-airlines-fbi-criminal-group

[13] Mao, R., Li, Y., Li, G., Petter Hildre, H., & Zhang, H. (2025). A systematic survey of digital twin applications: Transferring knowledge from automotive and aviation to maritime industry. IEEE Transactions on Intelligent Transportation Systems, 26(4), 4240-4259. https://doi.org/10.1109/tits.2025.3535593

[14] Marvakov, V. A., Huber, E., & Holzapfel, F. (2024). Developing modular vehicle and flight control management functions for eVTOL aircraft: From conceptual design to embedded design models. 2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC), 1-10. https://doi.org/10.1109/dasc62030.2024.10748868

[15] Merat, S., & Almuhtadi, W. (2025). A brief overview of the benefits of implementing quantum algorithms in factorizing cyber social engineering threats. Social Cyber Engineering and Advanced Security Algorithms, 226-249. https://doi.org/10.1201/9781003500698-22

[16] MITRE. (n.d.). ATT&CK. MITRE ATT&CK. https://attack.mitre.org/

[17] Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. Information, 13(3), 146. https://doi.org/10.3390/info13030146

[18] World Economic Forum. (2025, June 18). AI agents: The new frontier of cybercrime business must confront. weforum.org. https://www.weforum.org/stories/2025/06/ai-agent-cybercrime-business/

About Author:

Alex Mathew

Ph.D., CISA, CISSP, MCSA, CEH, CHFI, ECSA, CEI, CCNP etc.

- Is an Associate Professor in the Department of Cybersecurity at Bethany College (West Virginia, USA) and is widely recognized for his deep expertise in cybersecurity, cybercrime investigations, next-generation networks, data science, and IoT Azure solutions. His proficiency in security best practices, particularly in IoT, cloud systems, and healthcare IoT, is complemented by his comprehensive knowledge of industry standards such as ISO 17799, ISO 31000, ISO/IEC 27001/2, and HIPAA regulations. His credentials, including certifications in Cybersecurity and Data Science from Harvard University, further strengthen his expertise in the field.
- As a certified Information systems security professional (CISSP), Mathew's leadership is evident in his role as a consultant across international regions, including India, Asia, Cyprus, and the Middle East. His extensive two-decade career, distinguished by numerous certifications and over 100 scholarly publications, underscores his commitment to advancing the field. Mathew has been a pivotal force in organizing cybersecurity conferences and establishing incubation centers, contributing significantly to the academic and professional community.
- A highly sought-after speaker, Mathew's influence extends to international conferences where he shares his insights on cybersecurity, technology, and data science. His remarkable interpersonal skills and openness enhanced his ability to engage and inspire diverse audiences, further cementing his position as a leader in his field.

