



Keeping Pace with New Techniques through MITRE ATT&CK and Continuous Threat Intelligence Integration

ShivaDutt Jangampeta¹ & ShivaRaj Kumar Jakka²

¹Senior Manager of Security Engineering, JPMorgan Chase, Plano, USA.

²Splunk Consultant, Irving, USA

Abstract

The cybersecurity landscape is exceedingly dynamic, with new, more sophisticated cyber threats emerging as swiftly as technology advances. Today's most significant threats are social engineering, state-sponsored, ransomware, DDoS, insider threats, data breaches, and AI-powered attacks among others. The surge of these cyber threats has resulted in an equal response in the development of cybersecurity defenses. The future of seamlessly functioning cybersecurity lies in proactive techniques where businesses will not only respond to cyber threats but also foresee them. Consequently, security analysts are constantly devising new methods, techniques, and approaches to keep pace with hackers' tactics and techniques through the use of threat intelligence and cyber security frameworks like MITRE ATT&CK. This review discusses the ways organizations can keep pace with threat actors by leveraging the power of the MITRE ATT&CK framework.

Keywords

cyber threat, cyber threat landscape, MITRE ATT&CK, cybersecurity, cyberattacks, threat intelligence (TI), security analysts, Tactics, Techniques and Procedures (TTPs).

*Corresponding author: ShivaDutt Jangampeta¹

How to Cite: ShivaDutt Jangampeta & ShivaRaj Kumar Jakka. (2023). Keeping pace with new techniques through MITRE ATT&CK and continuous threat intelligence integration. *International Journal of Computer Science and Information Technology Research (IJCSITR)*, 4(2), 16-19.

Article ID: IJCSITR_2023_04_02_003

Article Link: https://ijcsitr.com/index.php/home/article/view/IJCSITR_2023_04_02_003/IJCSITR_2023_04_02_003



Copyright: © The Author(s), 2023. Published by IJCSITR Corporation. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution-Non-Commercial 4.0 International License (<https://creativecommons.org/licenses/by-nc/4.0/deed.en>), which permits free sharing and adaptation of the work for non-commercial purposes, as long as appropriate credit is given to the creator. Commercial use requires explicit permission from the creator.



I. INTRODUCTION

As shown in Figure 1 below, cyberattacks have become more complex and more prevalent, thus security analysts and organizations improve their ways of identifying, detecting, analyzing, and preventing them. However, understanding and combatting cyber threats is not a walk in the park [1]. In this context, the MITRE ATT&CK framework serves as a beacon of hope, clarity, and guidance. The comprehensive knowledge it provides makes ATT&CK more than just a model, but a prerequisite element of cybersecurity. Arguably, MITRE ATT&CK enables security teams to know the ways of adversaries [2].

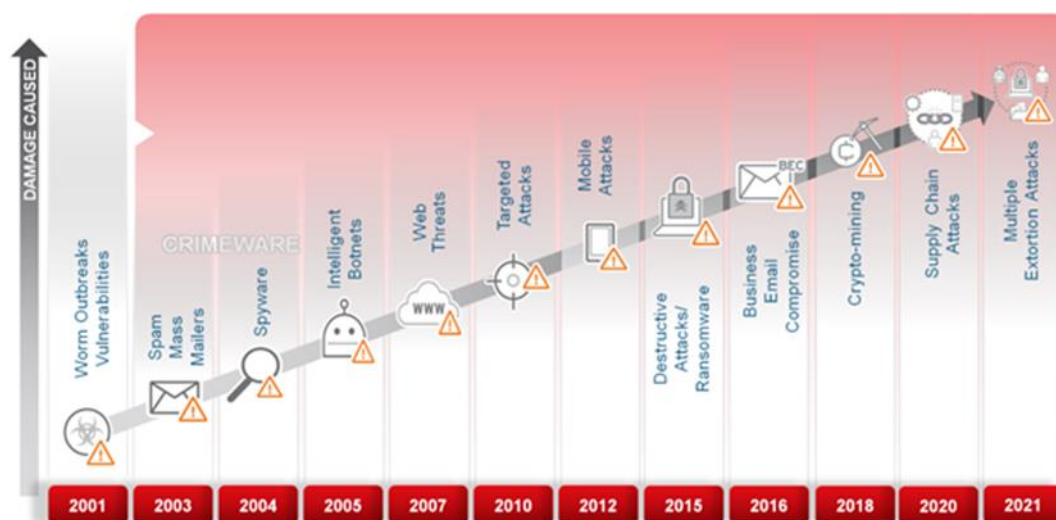


Figure 1. An illustration of threat evolution in the past two decades shows a surge in the threat prevalence.

2. What's MITRE ATT&CK and How Did It Started?

The adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework was developed by MITRE and is an organized knowledge base for threat actor behavior, reviewing the different stages of the cyberattack life cycle. MITRE ATT&CK framework emerged as a solution to address the dire need to fill the gap between conceptual cybersecurity knowledge and hands-on, practical intel [3]. Today, adversary techniques have grown in both numbers and complexity, with threat actors continually advancing their exploitation methods to target new vulnerabilities and outwit defensive measures. Conventional security controls usually fall short of dispensing the depth of comprehension needed to foresee and mitigate advanced threats. Consequently, ATT&CK was devised to address this challenge, to offer a systemized, all-inclusive database of familiar adversary behaviors and patterns, thoroughly classified into Tactics, Techniques, and Procedures (TTPs) [3]. It is used by cyber threat intelligence (CTI) teams, researchers, and security professionals as a vital tool, allowing a proactive and data-driven security posture.

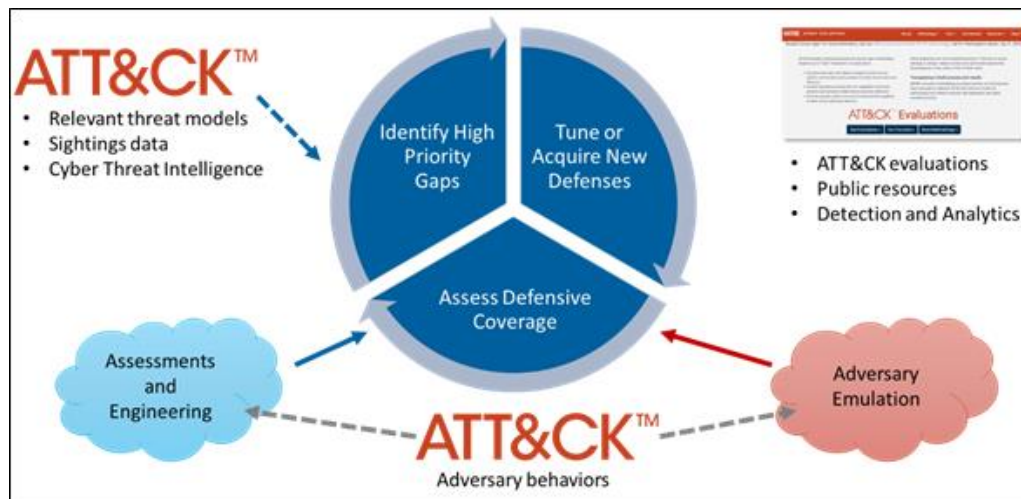


Figure 2. MITRE ATT&CT explained

A. Comprehensive Coverage of TTPs

ATT&CK showcases the cyber community's devotion to learning how to defend organizations against cyber threats. Its extensive coverage of TTPs is unrivaled, serving as a reflector to view the cyber threat environment and a map to traverse [4].

(i) **Framework's Depth and Breadth:** ATT&CK classifies adversary behavior into a model of tactics that detail the objectives a threat actor may need to achieve, and techniques describing the methods used to achieve those goals. Such an elaborate breakdown allows security analysts to understand attack anatomy, promoting a granular approach to security measures.

(ii) **Case Studies and Real-life Applications:** the framework draws on various sources, like security event reports, cyber threat intelligence feeds, or agile defense engagements. Security analysts can leverage this information to conduct attack simulations, assess their cybersecurity posture, and train their staff in identifying and responding to real-world cyber threats.

(iii) **Risk management and Threat modeling:** ATT&CK provides an exhaustive list of malicious actors' traits, allowing security experts to develop precise and stratified threat scenarios. The models can be used in the assessment of the severity of the risk, resource allocation, and protection of critical information [4].

3. Enhanced Threat Intelligence Through Real-Life Applications

MITRE ATT&CK highlights hands-on application and functional relevance by cutting across its role as a basic repository of hackers' TTPs. Focusing on practical utility significantly enhances TI capabilities, offering security analysts actionable insights that can be directly used in their defenses [4]. ATT&CK's inertia in real-life scenarios ensures that the insights generated are both all-inclusive and relevant, instantly applicable..

a) **Actionable Insights:** By analyzing TTPs observed in real-world security events, ATT&CK offers realistic visibility of the cyber threat environment, allowing security

teams to develop methods of bolstering their defenses.

b) **Bridge the Intelligence Gap:** the framework bridges the intelligence gap by contextualizing data regarding hackers' behavior within a rational framework directly connected with defense tactics. This contextualization process transforms unstructured information into a significant source of intel that can substantially help decision-making processes, surrounding tactical responses to prudent planning.

c) **Facilitates collaborative TI sharing:** sharing of threat intelligence among companies, industries, and countries can be eased by a systemized taxonomy and universal language. Cyber threats cut across industrial or geographical demarcations, making the collaborative aspect paramount [5]. The cybersecurity community can adopt a standard framework to describe adversary TTPs, enabling more efficient sharing of insights to collectively enhance their defense capabilities.

Empowers constant learning and adaptation: As security experts leverage ATT&CK to real-life situations, they acquire insights into the efficacy of different cybersecurity approaches. Learning and adapting can be imperatively significant in preventing threat actors by constantly refining their defense techniques.

CONCLUSION

MITRE ATT&CK framework has a remarkable impact on the way security analysts understand, liaise, and defend valuable, sensitive informational assets against threats, leveraging its all-inclusive coverage of hackers' TTPs, systemized analysis for specific defense plans, and fostering threat intelligence through real-life cases studies and applications. ATT&CK is a unified language that transcends institutional, industrial, and national boundaries and promotes a data-driven approach to cyber security. Providing exhaustive insights into threat actors' behavior and patterns, the framework enables security analysts to foresee and thwart cyber threats with efficacy, efficiency, and precision, enabling organizations to keep pace with new adversaries' techniques. Besides, the framework's focus on actionable applications guarantees the knowledge covered is both academically valuable and operationally relevant.

References

- [1] P. Prabakaran, Scalable Framework for Cyber Threat Situational Awareness, Self-Publisher, 2023.
- [2] C. A. Clark, Cybersecurity Incident Management Masters Guide, Amazon Digital Services LLC - Kdp, 2020.
- [3] R. Blair, Aligning Security Operations with the MITRE ATT&CK Framework: Level Up Your Security Operations Center for Better Security, Packt Publishing, 2023.
- [4] T. E. a. F. Dummies, Mitre ATT&CK For Dummies, AttackIQ Special Edition (Custom), Wiley, 2020.
- [5] R. Montasari, Artificial Intelligence and National Security, Springer International Publishing, 2022.