ASSIGNMENT 1- MITRE ATT&CK FRAMEWORK

MITRE ATT&CK (**Adversarial Tactics, Techniques, and Common Knowledge**)[1] is a matrix that defines the tactics, techniques, and procedures that adversaries will go through when trying to exploit and abuse systems that defenders are trying to protect. It mainly focusses on how adversaries penetrate networks and then move laterally, escalate privileges, and generally evade your defenses. Initially, it was designed for **Microsoft Windows** systems for improving detection of various harmful behavior. Later, it was expanded to other systems like **Linux**, **MacOS**, **Android**, **cloud-based systems**, and **industrial based control systems**. Organizations use this in order to find out defense fragility and then give priorities based on risk. According to **MITRE**, a **tactic**[2] is a huge description of attacker behavior and its type, and a **technique**[2] elaborates a detained analysis of specific type of the behavior in that tactic class.

MITRE ATT&CK consists of five different matrices based on the attacker's tactics and techniques:

- **PRE ATT&CK**[3]: Organized around an adversary's activity **before a launch attack**.
- **Enterprise – Linux**[3]: Looks after the execution of the attacks by **Linux**.
- **Enterprise – Windows**[3]: Looks after the execution of the attacks by **Windows**.
- **Enterprise – MacOS**[3]: Looks after the execution of the attacks by **MacOS**.
- **Mobile**[3]: Looks after the execution of the attacks by mobile **application**.

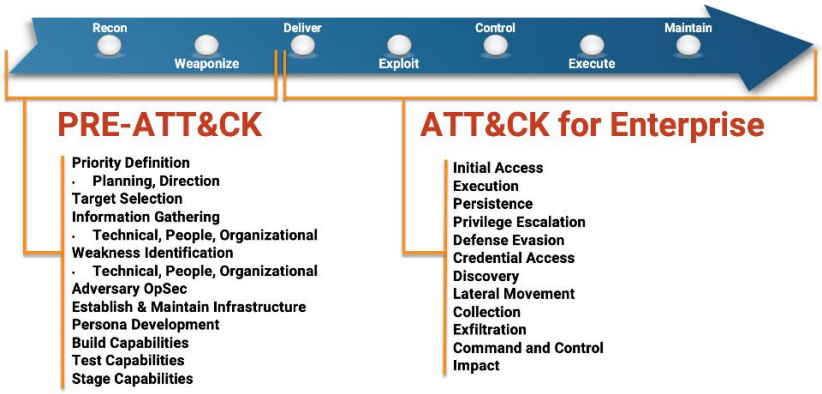


FIGURE 1: MATRICES OF MITRE ATT&CK
[Retrieved 10 September 2020, from https://medium.com/@socradar/whats-mitre-pre-att-ck-and-how-to-use-it-in-threat-intelligence-b78cfd5e6a90.]

MITRE ATT&CK was first started at **September 2013** with an intension of building a document of various techniques that the attackers use throughout various stages of cyberattacks[3]. The first ATT&CK model was focusing only for **Windows Environment** with some **96 techniques** and **9 tactics**. In the year **2017**, **MITRE** expanded the version for other operating systems and referred to as **ATT&CK for Enterprise**[4]. Later, several versions were developed with some added features like **cloud systems**, **mobile** and **ICS**[3] [4].

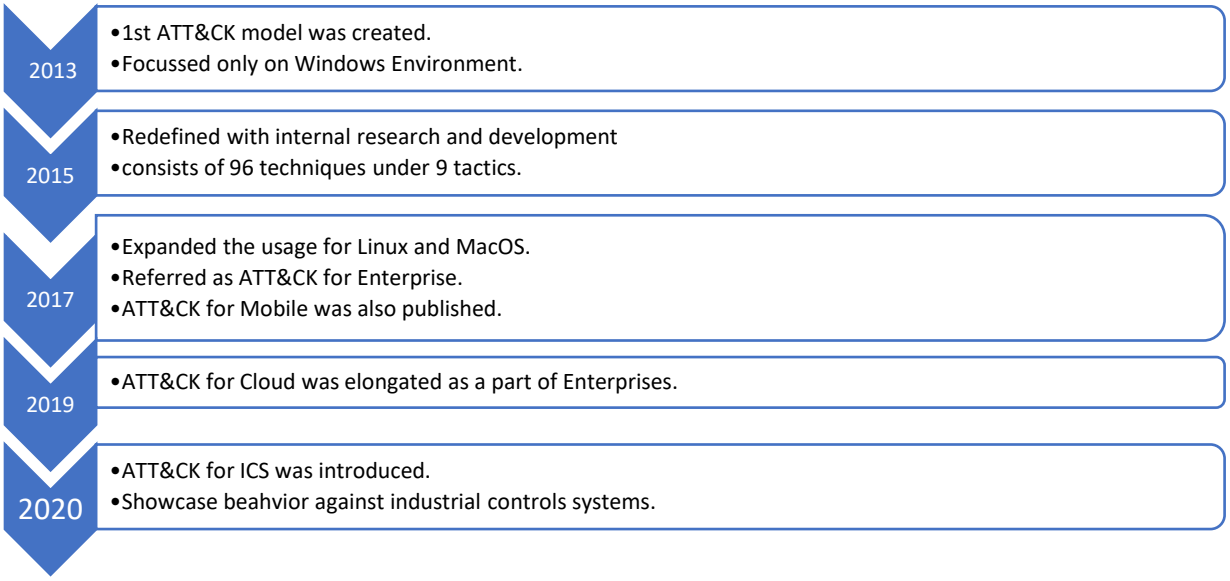
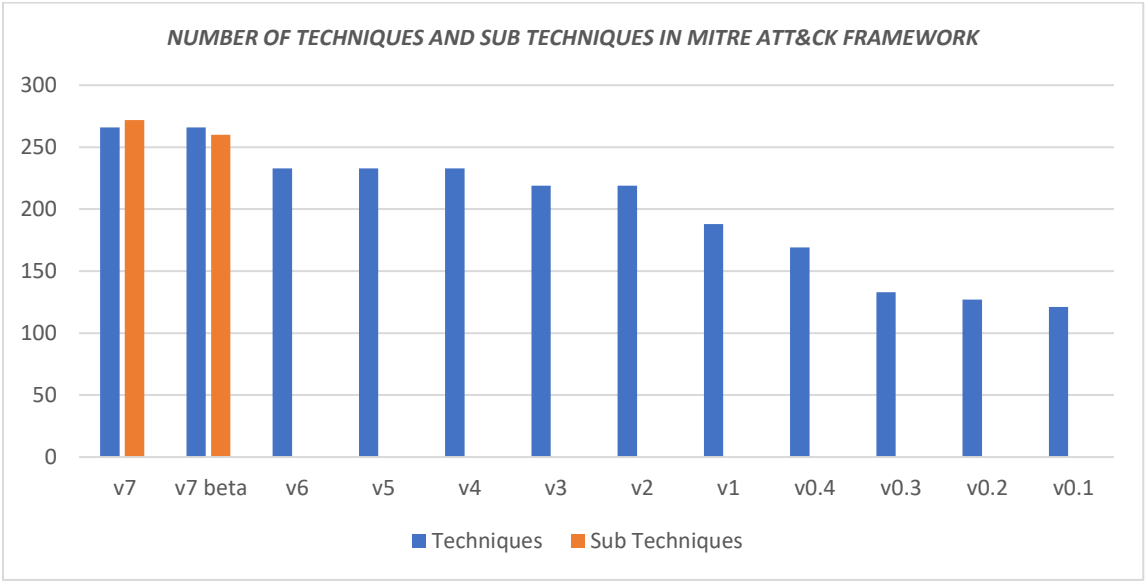


FIGURE 2: EVOLUTION OF MITRE ATT&CK FRAMEWORK

Latest version of MITRE ATT&CK framework was released on **8th July 2020**. The update involves the addition of new abstraction called the sub-techniques which are specific techniques. The new version consists of **256 techniques** and **272 sub-techniques**[2]. Previous versions of ATT&CK framework are still existing but the latest version would have additional sub-techniques. Below graph shows various versions with number of techniques and sub-techniques that has happened in past five years.



GRAPH 1: EVOLUTION OF MITRE ATT&CK FRAMEWORK
[Data retrieved from Versions of ATT&CK: MITRE ATT&CK®. (n.d.). September 10, 2020, from https://attack.mitre.org/resources/versions/]

The **ATT&CK matrix**[2][4] **structure** consists of **techniques** as **rows** and **phases in the attack chain** as **columns**. Framework users can evaluate any of the technique for gaining knowledge on **exploration of platforms, procedures, and detections**. It is possible for an attacker to involve **at least one technique** per tactic using **initial access** from **left** and **Command** on **right** from the matrix[4]. But there can be cases where multiple techniques can be utilized for one tactic. For example, in the case of **spear phishing**, the attacker can try on **attachment and link**.

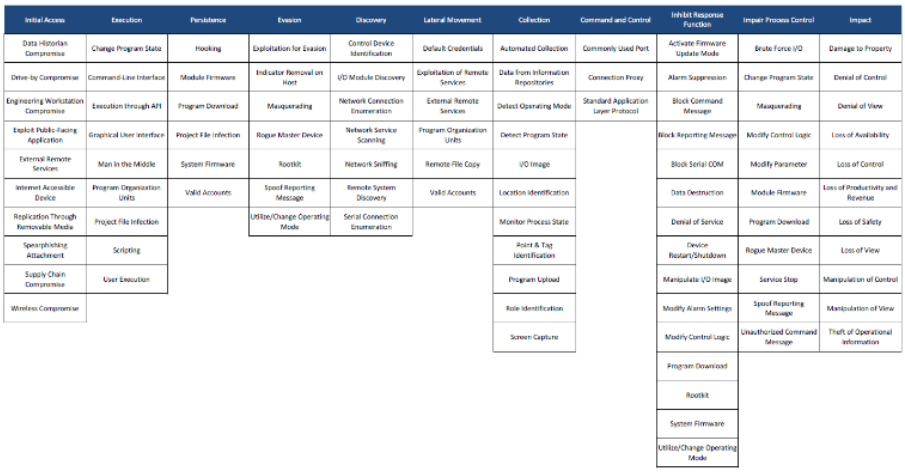


FIGURE 3: ATT&CK MATRIX
[Retrieved 10 September 2020, from https://medium.com/@socradar/whats-mitre-pre-att-ck-and-how-to-use-it-in-threat-intelligence-b78cfd5e6a90.]

There are few technologies that are been operated with the help of MITRE ATT&CK framework. **Recent Technologies** that are associated with MITRE ATT&CK are:

SNO	TECHNOLOGIES/PRODUCT	DESCRIPTION
1	BlackEnergy Malware Kit[5]	Useful for designing botnets in order to work on **Distributed Denial of Service (DDoS) attacks**,
2	Allwinner[6]	Supplies several processors that are useful in **Android tablets** and devices.
3	Attor[5]	**Windows-based platform** for utilizing several functionalities for targets.
4	Carrotball[7]	**FTP downloader** utility for using SYSCON.

TABLE 1: TECHNOLOGIES INVOLVING MITRE ATT&CK

The **ATT&CK Framework** is considered as a resource for understanding various **characteristics** and **techniques** associated with hackers against organizations. Some **important cases** for the MITRE ATT&CK framework includes:

1. **Prioritize** the threats in the attack chain of the organization.
2. Evaluate the **current telemetry** to each detection of the organization.
3. **Track** the attacker groups.

Several organizations tend to use MITRE ATT&CK framework for their advancements. They are:

1. **LogRhythm Labs**: **Brian Coulson** utilized MITRE ATT&CK by **aligning** the ATT&CK matrix with **log files like XML-Security, XML Systems** and so on. It seems to provide an effective way in detection techniques of logs[8] [10].

2. **Immersive Labs**: Immersive Labs joined with **cyber skills** liked with the tactics and techniques in ATT&CK framework. An ATT&CK map will show you where the **coverage is strong** along with **some improvements**[5] [9].
3. **Netskope**: Netskope utilized MITRE ATT&CK for developing contents on **cloud threats and techniques**. At Netskope, they focus on two analytical skills: **Detection and Analytics**[9] [10].
4. **Pcysys**: The main focus of the company is to showcase **solutions with cyber threats** with the help of an **automated, continuous networking platform** with MITRE ATT&CK framework[9] [10] [5].

REFERENCES

1. Maymí, F., Bixler, R., Jones, R., & Lathrop, S. (2017, December). Towards a definition of cyberspace tactics, techniques and procedures. In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 4674-4679). IEEE.
2. Al-Shaer, R., Spring, J. M., & Christou, E. (2020). Learning the Associations of MITRE ATT&CK Adversarial Techniques. *arXiv preprint arXiv:2005.01654*
3. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. *Technical report.*
4. Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., ... & Wolf, R. D. (2017). Finding cyber threats with ATT&CK-based analytics. *The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202*.
5. Alexander, O., Belisle, M., & Steele, J. (2020). MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy.
6. Gamba, J., Rashed, M., Razaghpanah, A., Tapiador, J., & Vallina-Rodriguez, N. (2020, May). An analysis of pre-installed android software. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 1039-1055). IEEE.
7. McCabe, A. (2020, March 12). The Fractured Statue Campaign: U.S. Government Agency Targeted in Spear-Phishing Attacks. Retrieved September 10, 2020, from https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/
8. Crowley, C. (2017). Future SOC: SANS 2017 Security Operations Center Survey. *May-2017*.
9. Raybourn, E. M. (2016). *A Metaphor for Immersive Environments: Learning Experience Design Challenges and Opportunities* (No. SAND2016-2988C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
10. Miloslavskaya, N. (2020). Stream Data Analytics for Network Attacks' Prediction. *Procedia Computer Science*, *169*, 57-62.