MITRE ATT&CK FRAMEWORK

Akshay Kaikottil

Johns Hopkins University

EN.650.683 Cybersecurity Risk Management

Tom McGuire

April 2022

Abstract

Emulating real world adversary scenarios and injecting real-world inspired activity into the network rapidly helps improve an organization's ability to detect threats. Adversary emulation is a sort of red red team team engagement in which mimics known threats by using threat intelligence to determine the red team's activities and behaviors. The purpose of this document is to discern the MITRE ATT&CK framework (The MITRE Corporation, 2015) which is a globally accessible knowledge base of adversarial techniques that can be used against specific platforms. This report focuses on the Tactics Techniques and Procedures used by HOLMIUM, a suspected Iranian threat group and develops mapping to the MITRE ATT&CK matrix.

Keywords: Adversary, Threat, Tactics, Techniques, Procedures.

Introduction

MITRE ATT&CK is a knowledge base and framework that composes cyber adversary behavior by considering several stages of the adversarial attack lifecycle as well as the platforms they are confirmed to attack. ATT&CK focuses on how external adversaries attack, compromise and operate within computer networks. The framework documents and prospects adversary tactics, techniques and procedures succeeding a network compromise.

ATT&CK was created out of a need to systematically categorize adversary behavior as part of conducting structured adversary emulation exercises within MITRE's FMX research environment (The MITRE Corporation et al., 2020). The original ATT&CK model was developed with the Windows enterprise environment in mind. It later grew to include Linux and macOS, and later domains such as mobile devices, cloud-based systems, and industrial control systems.

Groups are defined as intrusion sets, threat groups, actor groups, or campaigns that typically represent targeted, persistent threat activity (The MITRE Corporation et al., 2020). ATT&CK is mostly concerned with APT (Advanced Persistent Threat) organizations. Techniques are used by groups either directly or through software that can implement them. APT33, also known as Holmium or Elfin (*APT33, HOLMIUM, Elfin, Group G0064 | MITRE ATT&CK®*, 2018), is a suspected Iranian threat group. APT33 has targeted organizations – spanning multiple industries – headquartered in the United States, Saudi Arabia and South Korea since at least 2013. APT33 has shown particular interest in organizations in the

aviation sector involved in both military and commercial capacities, as well as organizations in the energy sector with ties to petrochemical production (O'LEARY et al., 2017).

Description

Use Cases of MITRE ATT&CK

The MITRE ATT&CK methodology may be used to find shortcomings in any organization's security. The framework can be applied in a variety of ways. MITRE ATT&CK provides six use cases (The MITRE Corporation et al., 2020):

1. **Adversary Emulation:** It's the process of assessing a technological domain's security by using cyber threat intelligence about individual adversaries and how they operate to reproduce the threat.
   Profiles for distinct adversary groups can be created using the ATT&CK framework. The blue team and hunting teams can also use these profiles to integrate and enhance defensive measures.

2. **Red Teaming:** Red teaming focuses on achieving the end goal of an operation without being detected in order to demonstrate the objective or operational influence of a successful breach. It's the act of conducting an exercise with a hostile attitude and without using known threat intelligence.
   To get over network-wide defensive countermeasures, the ATT&CK architecture can be utilized to construct red team strategies and organize operations. It can also serve as a research roadmap for developing new methods of performing certain tasks that are undetectable by standard defenses.

3. **Behavioral Analytics Development:** It is a method of attempting to leverage how an adversary communicates with a specific platform in order to evaluate and connect unusual behavior that is agnostic or unbiased to the use of sophisticated tools.
   The ATT&CK framework can be used to create and test behavioral analytics in order to detect adversarial action in a particular environment. The Cyber Analytics Repository (CAR) is one example of analytic development which could be used as a preliminary step for an organization to develop ATT&CK-based behavioral analytics. (The MITRE Corporation et al., 2020)

4. **Defensive Gap Assessment:** A defensive gap assessment enables a company to identify which parts of its enterprise have very little defenses and/or exposure. These disparities depict blind spots for potential vectors, enabling a malicious user to obtain unnoticed or unmitigated access to its networks.

   The ATT&CK framework is a prominent behavior-focused adversary model that could be used to assess existing defensive mechanisms, tools, monitoring, and mitigations within an organization's enterprise. The identified gaps can be used to prioritize investments for improving a cybersecurity strategy. Prior to purchasing, similar security products can be compared against common adversary behavior patterns to assess coverage.

5. **SOC Maturity Assessment:** The Security Operations Center (SOC) of a company is a vital component of many mid to big corporate environments that oversees the active threats against the company's network. Understanding the sophistication of a SOC is essential in determining its own efficiency.

   The ATT&CK framework is one such metric that may be used to assess how efficient a SOC is in detecting, analyzing, and responding to breaches. A SOC Maturity assessment, like a defensive gap assessment, focuses on how a SOC detects, understands, and adapts to foreign threats to a system over a period of time.

6. **Cyber Threat Intelligence Enrichment:** Understanding cyber threats and threat actor groups that influence cybersecurity is what cyber threat intelligence entails. It includes information on malware, tools, tactics, techniques, procedures, and other indicators associated with threats.

   The ATT&CK framework is beneficial for comprehending and capturing adversary group profile information from a behavioral stance that is unbiased to the group's tools. Recognizing how different groups use the same strategic behavior patterns allows investigators and researchers to focus on successful defensive lines that meet a wide range of dangers. ATT&CK's focused approach enhances threat reporting by categorizing activity that goes beyond normal signs.

ATT&CK Coverage

A concept of ATT&CK coverage is incorporated into ATT&CK use cases for defensive and red teaming. ATT&CK documents established adversary activity and is not designed to include a list of everything that must be tackled. One good example is Valid Accounts are handled, whether they be Local, Domain, or Cloud Accounts. The circumstances of their use may or may not indicate evil intent. It is vital to collect data about account usage, but without further context, it is difficult to flag malicious activities to an analyst. An opponent could use a variety of approaches to apply the techniques in ATT&CK. Always review threat intelligence on what tactics, sub-techniques, and procedures attackers have used to grasp the intricacies and how changes may alter how organizations assess coverage. ATT&CK is built on a set of tactics, methods, sub-techniques, and procedures that represent activities that adversaries can use to achieve their aims. When it comes to information security, the threats we face, emerging technologies, and the diversity of objective adversaries, we can't consider finishing a checklist as "done." (The MITRE Corporation et al., 2020)

Tactics, Techniques and Procedures

During an attack, tactics is a term used to describe the short-term tactical adversary goals. Tactics represent the “why” of an ATT&CK technique or sub-technique (The MITRE Corporation et al., 2020). Tactics are important categories for specific approaches since they encompass typical notations for activities that adversaries do during an endeavor. Each tactic has a definition that describes the category and acts as a guide to the approaches that are covered.

Techniques are the means through which opponents accomplish tactical goals. Techniques explain "how" an opponent accomplishes a tactical goal by performing a certain action. Techniques can also represent "what" an adversary obtains by executing an action. There may be various ways, or techniques, to attain tactical objectives, hence each tactic category contains multiple techniques. At a further simplifying techniques, sub-techniques outline more detailed methods through which opponents attain strategic objectives.

Procedures are a crucial element of the TTP concept and we cannot discuss tactics and techniques without referencing procedures. Procedures are the exact methods used by attackers for techniques or sub-techniques inside ATT&CK.

MITRE ATT&CK Matrix

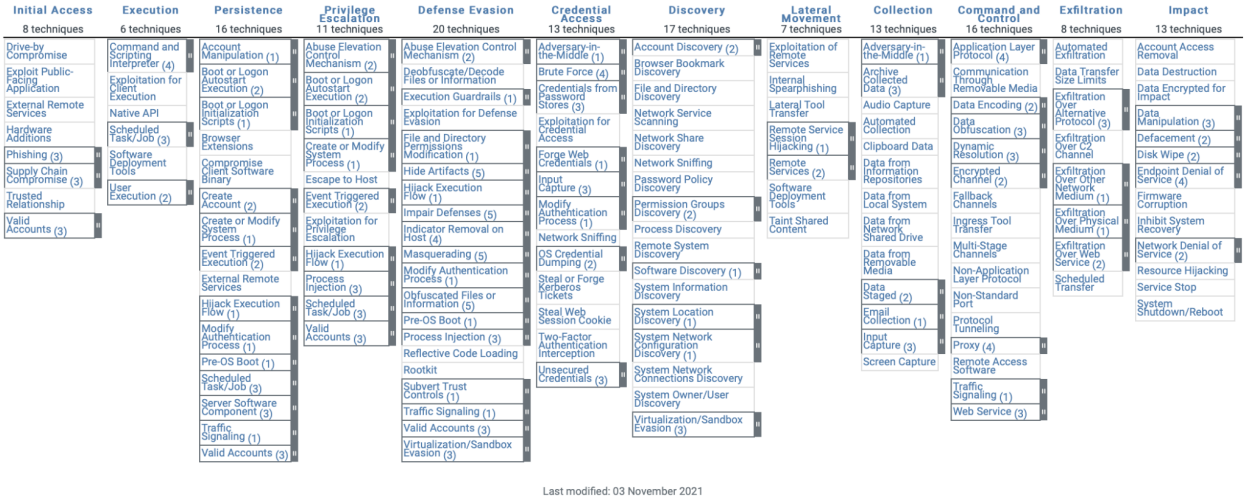

Figure 1. The ATT&CK for Linux Matrix

The ATT&CK Matrix depicts the correlation between tactics, techniques, and sub-techniques. Furthermore, some techniques can be broken into sub-techniques that explain at a deeper level how particular behavior patterns can be done. All matrices on the ATT&CK website are given a last revised timestamp, which functions as its version number.

Analysis

APT33

APT33 is an accomplished organization that has been conducting cyber espionage activities since at least 2013. It has been identified that APT33's actions are on behalf of the Iranian government. It is believed that APT33 operates in tactical espionage by targeting geographically varied businesses spanning numerous industries, based on identified targets.

To map APT33's TTPs, we employ the MITRE ATT&CK navigator and produce a graphical representation of the threat actor.This provides a simple way to gather Cyber Threat Intelligence from a threat actor and map it to MITRE ATT&CK for the creation of an Adversary Emulation strategy.

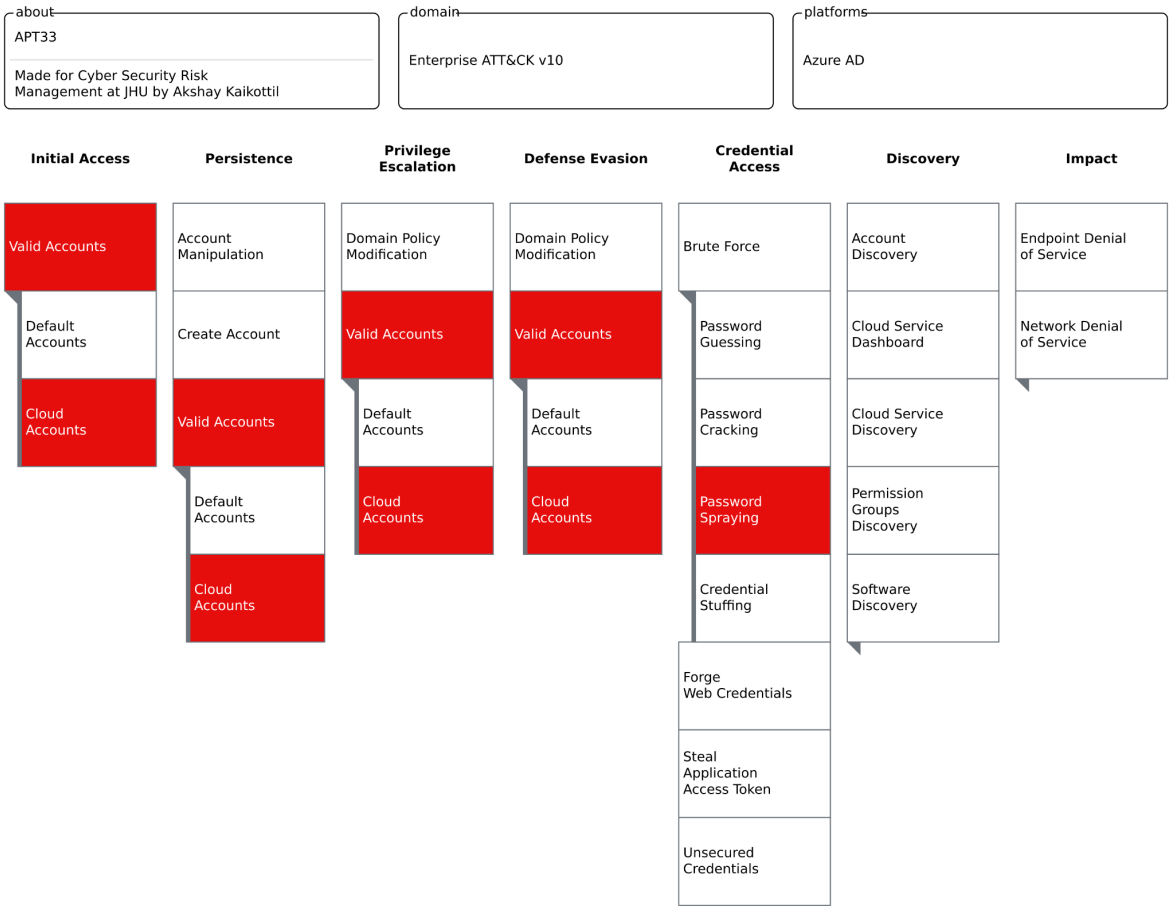

Figure 2. Mapping of APT33 Azure AD TTPs to MITRE ATT&CK Matrix

We then go through the Navigator and create a threat profile for APT33. For this we use the simplest method and create a table that contains the various tactics and techniques used by APT33.

Tactic	**Description**
Persistence	
Initial Access	
Privilege Escalation	
Defense Evasion	T1078.004 - Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
Credential Access	T1110.003 - Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials.

Table 1. APT33 Azure AD Threat Profile

To understand the threat better we also made a sample ATT&CK model relationship diagram.

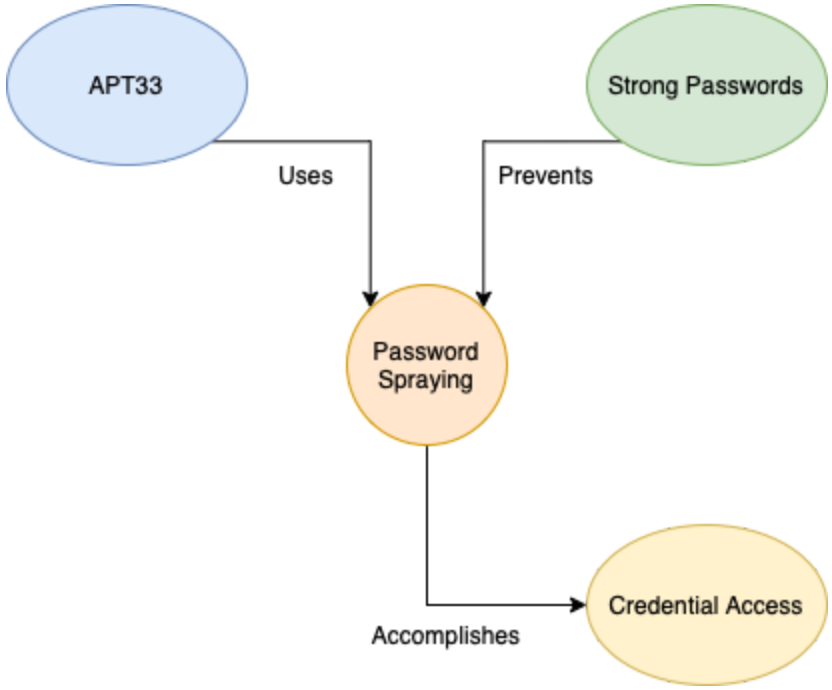

Figure 3. Password Spraying Relationship Model

Each high-level component of ATT&CK is linked to the others in various ways. The associations can be visualized.

Best Practices

Effective MITRE ATT&CK framework implementations should generate an accurate and reliable collection of mappings that can be utilized to construct adversary profiles, analyze activity trends, and be integrated into reports for detection, response, and mitigation. In order to accomplish goals it is always necessary that one take a systematic approach. Below are some of the best practices that are recommended while applying the MITRE ATT&CK framework:

1. **Find the behavior:** Try to identify how the initial compromise was achieved as well as how the post- compromise activity was performed.
2. **Research the behavior:** Try to figure out how the original compromise was reached and how the post-compromise action was carried out.
    a. Look at the original reports to understand how the behavior was inferred.

   b. Not all behaviors can translate into techniques and sub-techniques. But they can always provide more understanding on the overall adversary behavior.
   c. Search for key terms on the ATT&CK website to help identify the behaviors.
3. **Identify the tactics:** Identify the adversary tactics and the flow of the attack.
   a. Examine the tactic descriptions to see if the observed behaviors can be translated into a specific tactic.
   b. Identify all of the tactics in the report.
4. **Identify the techniques:** Study the technical details of how the enemy attempted to attain their objectives.
   a. Evaluate the conduct described in the report to the ATT&CK techniques specified underneath the indicated tactic.
   b. Be mindful that many approaches may be applied to the same behavior at the same time.
   c. Do not suppose or conclude that a technique was employed unless it is plainly outlined or that is the only technical possibility for the behavior to have transpired.
   d. To uncover possible strategies that fit the described behavior, look for technical details, keywords, or command lines.
   e. Check that the techniques correspond to the right tactics.
   f. Consider techniques and sub-techniques as components of an adversary's armory, rather than as separate operations.
5. **Identify the sub-techniques:** Analyze sub-technique definitions to see if they correspond to the information in the report.
   a. Read the sub-technique descriptions carefully to understand the differences between them.
   b. In cases where the parent of a sub-technique aligns to multiple tactics, make sure to choose the appropriate tactic.
   c. Please notify the ATT&CK team if you are observing a new technique or sub-technique.

6. **Compare your results with other analysts:** Working on mappings with other analysts adds a variety of viewpoints and helps provide other perspectives, which can enhance awareness about potential analyst biases.

Comparative Study of Similar Frameworks

A framework in cybersecurity is a system of standards, guidelines, and best practices for controlling risks in today's digital age. A cybersecurity framework provides adaptable, consistent, and cost-effective approaches to increase a company's security and resilience. Most security frameworks are tailored to certain enterprises and groups, with advice tailored to their specific needs and ensuring compliance. To choose a framework, we must first evaluate which one best meets one's needs or what the industry standard is.

1. **Lockheed Martin Kill Chain:** “The Cyber Kill Chain framework is part of the Intelligence Driven Defense model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective” (Lockheed Martin, n.d.).

   The ATT&CK architecture is a tactic matrix that is not constrained by a certain order of operations, whereas Cyber Kill has an organized linear series of steps. The military notion of a kill chain model is applied to a cyberattack in cyber kill. Its purpose is to assist defenders in strengthening their defenses by evaluating an attacker's tactics and stopping the attack by interrupting the kill chain at every phase. In the MITRE ATT&CK framework, you are provided with a more fluid means of analyzing what an adversary might do and being better at avoiding it.
2. **NIST Cybersecurity Framework:** The National Institute of Standards and Technology's (NIST) Cybersecurity Framework is a collection of best practices, standards, and guidelines that can help an organization improve its cyber defenses. The NIST framework is divided into five governing areas that outline how to secure, identify, detect, respond, and recover information. These five domains contain various traits and abilities, but they do not immediately explain how to investigate a cyber security threat or give analytic indicators for testing detection methods. ATT&CK, contrary to NIST, is a holistic system that gives a common catalog of tactics, techniques, and procedures that may be used in real-world scenarios.
3. **Diamond Model:** Analysts use the Diamond Model to hunt, pivot, analyze, group, and structure intrusion prevention. The adversary, infrastructure, capability, and victim are the four main

aspects of intrusion, and the Diamond Model focuses on the relationships and characteristics of these four features. From both the attack and defense perspectives, ATT&CK maps and indexes virtually everything related to an infiltration. ATT&CK contains information on threat organizations, their tactics, and even references and instances. Red teams can emulate ATT&CK-mapped attack scenarios, while blue teams can test them. ATT&CK now has information about cybersecurity providers, their products, and their skills thanks to the Assessments. None of them are possible with the Diamond Model.

Conclusion

For APT33, we ingested threat intelligence, extracted TTPs, and devised an adversary emulation strategy. Cyber threat intelligence is critical to a company's ability to defend against emerging attacks. It contains details on the tools, strategies, and procedures employed by several active threat actor organizations. ATT&CK has been embraced by a variety of disciplines, including threat intelligence, intrusion detection, threat hunting, security engineering, risk assessment and red teaming.

The capacity of the ATT&CK framework to provide an uniform, widely accessible global language, as well as information into attackers' behaviors, has resulted in its growing popularity among enterprises looking to integrate threat intelligence and increase their cyber resilience. Cyber threat information provided in MITRE ATT&CK will give enterprises a window into adversaries' strategies, allowing them to think like an adversary and make informed decisions to prevent harmful, targeted attacks before they happen.

References

1. *Advanced persistent threat*. (n.d.). Wikipedia. Retrieved April 19, 2022, from https://en.wikipedia.org/wiki/Advanced_persistent_threat
2. *APT33, HOLMIUM, Elfin, Group G0064 | MITRE ATT&CK®*. (2018, April 18). MITRE ATT&CK®. Retrieved April 19, 2022, from https://attack.mitre.org/groups/G0064/
3. CISA. (2021, June). Best Practices for MITRE ATT&CK® Mapping. https://www.cisa.gov/uscert/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf
4. Cosio, F. (2022, January 10). *Spot the difference: MITRE Framework vs. Lockheed Martin Kill Chain (Cyber Kill Chain®)*. Brier & Thorn. Retrieved April 23, 2022, from https://www.brierandthorn.com/post/spot-the-difference-mitre-framework-vs-lockheed-martin-kill-chain-cyber-kill-chain
5. CyCraft Technology Corp. (2020, June 30). *CyCraft Classroom: MITRE ATT&CK vs. Cyber Kill Chain vs. Diamond Model*. Medium. Retrieved April 23, 2022, from https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f
6. *Getting Started with ATT&CK – MITRE ATT&CK*. (n.d.). Medium. Retrieved April 21, 2022, from https://medium.com/mitre-attack/getting-started/home
7. Greenberg, A. (2019, November 20). *Iran's APT33 Hackers Are Targeting Industrial Control Systems*. WIRED. Retrieved April 23, 2022, from https://www.wired.com/story/iran-apt33-industrial-control-systems/
8. Lockheed Martin. (n.d.). *Cyber Kill Chain®*. Lockheed Martin. Retrieved April 23, 2022, from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
9. The MITRE Corporation. (n.d.). *Matrix - Enterprise | MITRE ATT&CK®*. MITRE ATT&CK®. Retrieved April 23, 2022, from https://attack.mitre.org/matrices/enterprise/
10. The MITRE Corporation. (2015). *MITRE ATT&CK FRAMEWORK*. MITRE ATT&CK®. Retrieved April 19, 2022, from https://attack.mitre.org
11. The MITRE Corporation. (2021, February 03). *ATT&CK® Navigator*. mitre att&ck. Retrieved April 23, 2022, from https://mitre-attack.github.io/attack-navigator/

12. The MITRE Corporation, Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020, March 3). MITRE ATT&CK®: Design and Philosophy. *MITRE ATT&CK®*. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
13. O'LEARY, J., KIMBLE, J., VANDERLEE, K., & FRASER, N. (2017, September 20). *Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware*. Mandiant. Retrieved April 20, 2022, from https://www.mandiant.com/resources/apt33-insights-into-iranian-cyber-espionage
14. Orchilles, J. (2020, June 18). *SCYTHE Library: #ThreatThursday - APT33*. Scythe.io. Retrieved April 23, 2022, from https://www.scythe.io/library/threatthursday-apt33
15. Poston, H. (2020, November 11). *Use cases for implementing the MITRE ATT&CK® framework - Infosec Resources*. Infosec Resources. Retrieved April 23, 2022, from https://resources.infosecinstitute.com/topic/use-cases-for-implementing-the-mitre-attck-framework/
16. Ryerse, J. (2020, October 5). *The importance of a cybersecurity framework | 2020-10-01*. Security Magazine. Retrieved April 23, 2022, from https://www.securitymagazine.com/articles/93509-the-importance-of-a-cybersecurity-framework
17. Seals, T. (2019, November 14). *APT33 Mounts Focused, Highly Targeted Botnet Attacks Against U.S. Victims*. Threatpost. Retrieved April 23, 2022, from https://threatpost.com/apt33-mounts-targeted-botnet-attacks-us/150248/