WEEK 2
MITRE ATT&CK

TIMOTHY SEWE OGODE(CSSA0423076)

CYBER SHUJAA

2.1 MITRE ATT&CK

Table of Contents

2.1 MITRE ATT&CK

1. INTRODUCTION

MITRE, a renowned organization in the realm of cybersecurity, stands as a pioneering force dedicated to bolstering digital defence and resilience in an ever-evolving threat landscape. With its extensive expertise and collaborative approach, MITRE actively engages with both government and industry to tackle complex challenges head-on. By leveraging its vast knowledge, cutting-edge research, and practical solutions, MITRE empowers organizations to proactively identify vulnerabilities, mitigate risks, and fortify their cyber defences, ultimately safeguarding critical infrastructures and protecting sensitive information from malicious actors. In this report we will focus mostly on ATT&CK®(Adversarial Tactics, Techniques, and Common Knowledge) Framework, CAR (Cyber Analytics Repository) Knowledge Base, ENGAGE (sorry, not a fancy acronym), D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defence), AEP (ATT&CK Emulation Plans).

2. BASIC TERMINOLOGY

APT(advanced persistent threat) refers to a team/group (threat group), nation-state group, or even government that conducts persistent assaults on companies and/or nations. These APT organizations employ a few approaches that, with the proper implementations, may be easily identified. TTP(Tactics, Techniques, and Procedures) , The Tactic is the adversary's goal or objective, the Technique is how the adversary achieves the goal or objective, the Procedure is how the technique is executed.

3. ATT&CK FRAMEWORK

The MITRE ATT&CK framework has emerged as a seminal resource in the field of cybersecurity, offering an unparalleled and comprehensive framework for understanding and responding to cyber threats. Designed to capture the tactics, techniques, and procedures employed by adversaries during various stages of a cyberattack, ATT&CK provides organizations with a structured approach to enhancing their defensive capabilities. By mapping out the entire attack lifecycle and cataloguing adversary behaviours, ATT&CK enables security teams to proactively identify and counteract potential threats, bolstering their resilience and ensuring effective incident response. With its widespread adoption and continuous updates, the MITRE ATT&CK framework has become an indispensable tool for organizations seeking to navigate the intricate landscape of cybersecurity with precision and efficacy.

Questions

Besides blue teamers, who else will use the ATT&CK Matrix?
red teamers

What is the ID for this technique?
T1566

Based on this technique, what mitigation covers identifying social engineering techniques?
User Training

What are the data sources for Detection? (format: source1,source2,source3 with no spaces after commas)
Application Log,File,Network Traffic

What groups have used spear-phishing in their campaigns? (format: group1,group2)
Axiom,GOLD SOUTHFIELD

2.1 MITRE ATT&CK

Based on the information for the first group, what are their associated groups?
Group 72

What software is associated with this group that lists phishing as a technique?
Hikit

What is the description for this software?
Hikit is malware that has been used by Axiom for late-stage persistence and exfiltration after the initial compromise

This group overlaps (slightly) with which other group?
Winnti Group

How many techniques are attributed to this group?
15

4. CAR KNOWLEDGE BASE

The Cyber Analytics Repository, often referred to as CAR, is a valuable resource in the field of cybersecurity that offers a collection of pre-built analytics and detection rules. Created and maintained by the cybersecurity community, CAR provides security analysts and practitioners with a curated repository of proven and tested analytics that can be utilized to detect and respond to various cyber threats. These analytics encompass a wide range of techniques, including behavioural analytics, machine learning algorithms, and signature-based detection rules. By leveraging CAR, organizations can benefit from a wealth of community-driven knowledge, accelerating their ability to identify and mitigate security incidents effectively. With its collaborative nature and continuous updates, the Cyber Analytics Repository serves as an asset in the pursuit of building robust cybersecurity defences.

Questions

For the above analytic, what is the pseudocode a representation of?
Splunk search
What tactic has an ID of TA0003?
Persistence
What is the name of the library that is a collection of Zeek (BRO) scripts?
BZAR
What is the name of the technique for running executables with the same hash and different names?
Masquerading
Examine CAR-2013-05-004, besides Implementations, what additional information is provided to analysts to ensure coverage for this technique?
Unit Tests

5. MITRE ENGAGE

MITRE Engage is a dynamic platform established by MITRE, a renowned organization in the field of cybersecurity, to foster collaboration and knowledge sharing among cybersecurity professionals. Designed to bridge the gap between government, industry, and academia, MITRE Engage provides a space for cybersecurity experts to connect, exchange ideas, and collaborate on pressing cybersecurity challenges. Through forums, working groups, and interactive discussions, MITRE Engage facilitates the

sharing of best practices, emerging trends, and innovative solutions in cybersecurity. By promoting a culture of collaboration and collective problem-solving, MITRE Engage aims to advance the field of cybersecurity and drive impactful change in the ever-evolving digital landscape.

Questions

Under Prepare, what is ID SAC0002?
Persona Creation
What is the name of the resource to aid you with the engagement activity from the previous question?
PERSONA PROFILE WORKSHEET
Which engagement activity baits a specific response from the adversary?
Lures
What is the definition of Threat Model?
A risk assessment that models organizational strengths and weaknesses

6. D3FEND

D3FEND stands for Detection, Denial, and Disruption Framework Empowering Network Defence. D3FEND is a comprehensive cybersecurity framework developed by MITRE that focuses on active cyber defence techniques and strategies. Building upon the widely adopted MITRE ATT&CK framework, D3FEND provides organizations with a structured approach to enhancing their defensive capabilities and mitigating cyber threats.

Questions

What is the first MITRE ATT&CK technique listed in the ATT&CK Lookup dropdown?
Data Obfuscation
In D3FEND Inferred Relationships, what does the ATT&CK technique from the previous question produce?
Outbound Internet Network Traffic

7. ATT&CK EMULATION PLANS

Provide detailed guidance and methodologies for simulating real-world cyber attack scenarios. Emulation Plans assist organizations in evaluating their defensive capabilities by replicating adversary behaviours and tactics within a controlled environment. These plans outline step-by-step instructions, tools, and techniques to emulate specific adversary techniques and tactics mapped to the ATT&CK framework.

Questions

In Phase 1 for the APT3 Emulation Plan, what is listed first?
C2 Setup
Under Persistence, what binary was replaced with cmd.exe?
sethc.exe
Examining APT29, what C2 frameworks are listed in Scenario 1 Infrastructure? (format: tool1,tool2)
Pupy,Metasploit Framework
What C2 framework is listed in Scenario 2 Infrastructure?
PoshC2
Examine the emulation plan for Sandworm. What webshell is used for Scenario 1? Check MITRE ATT&CK for the Software ID for the webshell. What is the id? (format: webshell,id)
P.A.S.,S0598

2.1 MITRE ATT&CK

8. ATT&CK and THREAT INTELLIGENCE

The information, or TTPs, attributed to the opponent is known as threat intelligence. As defenders, we may choose the best defensive plan by employing threat intelligence. In addition to leveraging already-available threat data, large businesses may have an internal team whose main goal is to acquire threat intelligence for other teams inside the firm. Some of this threat intelligence is accessible through open source or by subscribing to a vendor like CrowdStrike. In contrast, many defenders in certain companies do several responsibilities and must take time away from those positions to concentrate on threat intelligence.

Questions

What is a group that targets your sector who has been in operation since at least 2013?
APT33
As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it?
Cloud Accounts
What tool is associated with the technique from the previous question?
Ruler
Per the detection tip, what should you be detecting? (format: phrase1 or phrase2)
multi-factor authentication
What platforms does the technique from question #2 affect?
Azure AD, Google Workspace, IaaS, Office 365, SaaS

9. CONCLUSION

In conclusion, MITRE plays a vital role in the cybersecurity landscape through its innovative frameworks and collaborative platforms. The MITRE ATT&CK framework provides organizations with a comprehensive understanding of adversary tactics, enabling them to bolster their defences and proactively respond to evolving threats. Additionally, the Cyber Analytics Repository and ATT&CK Emulation Plans offer valuable resources for enhancing detection capabilities and simulating realistic attack scenarios. By integrating threat intelligence with the ATT&CK framework, organizations can further strengthen their defences and stay ahead of adversaries. With MITRE's contributions, the cybersecurity community is empowered to share knowledge, collaborate, and collectively build robust defences against the ever-present and sophisticated cyber threats of today's digital world. **LINK**