SIMULATION & ANALYSIS OF CYBER ATTACKS USING MITRE ATT&CK FRAMEWORK

TEAM
CIPHERGUARD

UMER

TALHA

JAWAD

UBAID

AHSAN

Table of Content

Simulation and Analysis of Attacks Using MITRE ATT&CK Framework

Project Title: Simulation/Analysis of APT Attack Using MITRE ATT&CK Framework

Team Name: CipherGuard

Team Members:

- Ubaid
- Umer
- Talha
- Jawad
- Ahsan

Introduction to MITRE ATT&CK:

MITRE ATT&CK is an open-source framework that documents the tactics and techniques used by adversaries. The acronym stands for *Adversarial Tactics, Techniques, and Common Knowledge*. This framework was developed to provide a deep understanding of cyberattacks, enabling security professionals to simulate and analyse real-world attack scenarios. Each technique within the framework is assigned a unique ID, which facilitates documentation, investigation, and the sharing of threat intelligence. It is a highly valuable resource for cybersecurity experts, Security Operations Centre (SOC) analysts, and threat hunters worldwide.

Importance of MITRE ATT&CK in Cybersecurity:

MITRE ATT&CK helps organizations understand how attackers think and operate. By leveraging this framework, security teams can enhance their detection and response strategies. It enables them to identify security gaps and strengthen their defences accordingly. The framework is also highly valuable for red teaming, threat intelligence, and incident response activities. By providing a structured and evidence-based approach, MITRE ATT&CK enables organizations to effectively counter cyber threats.

Case Studies:

To better understand **MITRE ATT&CK**, several hypothetical scenarios have been developed, which also provide insights into the attacker's mindset.

Scenario 1 (Freelancer):

Attack Scenario Description:

Target: A freelance graphic designer working from home.

Motive: The attacker's objective was to steal the client's confidential data and generate profit through a ransomware attack.

Scenario:

A freelance graphic designer received an email purportedly from Adobe Support. The email claimed that a free plugin was available to enhance Photoshop's capabilities. It appeared highly professional and included Adobe's branding, making it look authentic. Believing it to be genuine, the freelancer downloaded and installed the plugin. Unbeknownst to them, the plugin contained malware that granted the attacker remote access to their computer.

Once the attacker gained control of the system, they scanned the client's project files and subsequently encrypted all of them. The attacker then left a ransom note demanding $500 in Bitcoin in exchange for restoring access to the files. Since the freelancer did not have a recent backup, they were left with only two options:

1. Pay the ransom.
2. Permanently lose the important client data.

Threat Actor Type:

- **Cybercriminal** (not affiliated with any government entity).
- The primary motive is financial gain.
- Uses phishing and malware to harm individuals and organizations.

Tactics and Techniques:

In this scenario, the attacker sends a fake email to the freelancer containing a malicious attachment, which the freelancer downloads and executes on their device. This action triggers the malware, enabling the attacker to gain elevated privileges. The malware exploits system misconfigurations to escalate privileges without the user's consent.

Phase	Technique Used	MITRE ATT&CK ID	Description
Initial Access	Phishing: Spearphishing Attachment	T1566.001	The attacker sends a fake email containing a malicious plugin or download link.
Execution	User Execution: Malicious File	T1204.002	The freelancer downloads and executes the plugin, which triggers the malware.
Privilege Escalation	Exploitation for Privilege Escalation	T1068	The malware then exploits an operating system or application vulnerability to obtain elevated privileges.
		T1548.002	The malware bypasses Windows User Account

	Abuse Elevation Control Mechanism: Bypass UAC		Control (UAC) by tricking the system or exploiting misconfigurations, allowing it to gain elevated privileges without the user's consent.
Persistence	Remote Access Tool or Backdoor Installation	T1059	The attacker installs a tool to maintain persistent access to the system.
Defence Evasion	Encrypted Payload	T1027	The attacker disguises the plugin to evade detection by antivirus software.
Discovery	File and Directory Discovery	T1083	The attacker scans the system to locate the freelancer's important project files.
Collection	Data from Local System	T1005	The attacker selects specific files with the intent to encrypt them.
Command and Control	Application Layer Protocol (HTTP/S)	T1071.001	The malware on the freelancer's computer communicates with the attacker's command-and-control (C2) server.
Impact	Data Encrypted for Impact (Ransomware)	T1486	The attacker encrypts the important files.

Individual Scenario – Detection & Mitigation:

Detection Techniques:

- **SIEM (Security Information and Event Management):**
  SIEM alerts can detect suspicious file executions, privilege escalation attempts, and unusual user behavior.
- **EDR (Endpoint Detection and Response):**
  Detects malicious plugins, suspicious PowerShell activity, and unauthorized access attempts.

Log Monitoring:

- **Email logs:** To trace spearphishing attempts.
- **App logs:** Record instances of plugin installation or execution.
- **Windows Event Logs:** Track UAC bypass activities and privilege changes.

Mitigation Recommendations:

MITRE ID	Technique	Description
M1036	Account Use Policies	Implement strict policies for user accounts, particularly those with administrative privileges.
M1054	Software Configuration	Disable the unnecessary use of plugins or macros.
M1017	User Training	Provide freelancers with training to recognize phishing emails and potentially malicious attachments.
M1032	Multi-Factor Authentication	Make multi-factor authentication (MFA) mandatory for sensitive access.
M1047	Application Isolation	Execute unknown files within a sandbox environment.

Scenario 2 (Medium Level Company):

Attack Scenario Description:

Target: A medium-sized digital marketing company with 30–40 employees.

Motive: The attacker's objective was to steal client campaign data and staff login credentials and to extort money through a ransomware attack.

Scenario:

A medium-sized digital marketing agency received an email that appeared to be from Google Ads Support. The email stated that their account was being suspended due to a policy violation and instructed the marketing manager to click a link to verify the account immediately. Without hesitation, the manager clicked the link, which led to a fraudulent Google login page. Believing it to be legitimate, they entered their actual username and password, which were instantly transmitted to the attacker.

Using these stolen credentials, the attacker gained access to the company's Google Workspace account, viewed sensitive client information, and installed a malicious browser extension on the manager's system. This malware allowed the attacker to move freely within the company's network, harvest credentials from other staff members, and encrypt client folders. The attacker then demanded a ransom of $2,000 in Bitcoin.

Since the company lacked both recent backups and proper network segmentation, they had no alternative but to pay the ransom. Otherwise, years of work would have been lost.

Threat Actor Type: A cybercriminal group motivated solely by financial gain, utilizing phishing, credential theft, network intrusion, and ransomware deployment.

Tactics and Techniques:

A medium-sized digital marketing agency received a fraudulent email claiming to be from Google Ads Support. The email stated that their account had been suspended and required verification. The manager clicked the provided link, which led to a fake login page. After entering their Google credentials, the attacker used them to access the company's account, install a malicious browser extension, move laterally within the internal network, and ultimately launch a ransomware attack.

Phase	Technique Used	MITRE ATT&CK ID	Description
Initial Access	Phishing (Spearphishing Link)	T1566.002	The attacker sent a fake Google Ads email containing a phishing link.
Credential Access	Credential Harvesting	T1556.002	The manager entered their credentials on the fake login page.
Persistance	Browser Extension	T1176	The attacker installed a malicious extension in the manager's browser.
Discovery	Account Discovery	T1087.002	Through Google Workspace, the attacker explored user and email data.

Lateral Movement	Internal Spearphishing / Reuse Credentials	T1550.002	Using the harvested credentials, the attacker also gained access to other staff accounts.
Impact	Data Encrypted for Impact (Ransomware)	T1486	The attacker encrypted the clients' folders and demanded a ransom of $2,000 in Bitcoin.

Medium Company Scenario – Detection & Mitigation:

Detection Techniques:

- **SIEM:** Fake login attempts, suspicious browser extensions, and lateral movement can be detected.
- EDR: Malicious extension installation, credential harvesting, and ransomware execution can be detected.

Log Monitoring:

- **Email Logs:** To trace the phishing email.
- **Browser Logs:** Malicious extension activity.
- **Google Workspace Logs:** To trace unauthorized access and data downloads.
- **File Logs:** To monitor encryption activity.

Mitigation Recommendations:

MITRE ID	Technique	Description
M1032	Multi-Factor Authentication	Enable multi-factor authentication (MFA) on Google Workspace and other sensitive applications.
M1017	User Training	Provide employees with training to recognize phishing attempts and fake websites.
M1049	Antivirus/Antimalware	Implement strong endpoint protection capable of detecting malicious extensions.
M1030	Network Segmentation	Keep sensitive client folders in a separate network segment.
M1053	Data Backup	Maintain regular and offline backups.

Scenario 3 (Big Enterprise Company):

Attack Scenario Description:

Target: A multinational IT company with over 500 employees.

Motive: The attacker's goal was to infiltrate the company's internal network, steal their Research and Development (R&D) data, and later sell it to a competitor. Additionally, the attacker deployed ransomware to disrupt the company's systems.

Scenario:

A senior software engineer at the company received an email that appeared to be from a job recruitment agency. The email stated that their resume had been shortlisted by a major tech company and requested them to review a PDF file to proceed with the application. Upon downloading the PDF, which contained macro-enabled malicious code, the attacker gained silent access to the company's internal systems.

The attacker first compromised the engineer's system and then moved laterally within the network, eventually reaching the domain controller and other servers. They extracted proprietary R&D data from the company and uploaded it to a remote server. Subsequently, the attacker deployed ransomware across multiple company systems, encrypting all user files and rendering the systems unusable. A ransom demand of $100,000 in Bitcoin was issued.

Although the company had some backups, they were outdated and did not contain the latest R&D data. As a result, the company was compelled to pay the ransom to avoid losing critical intellectual property. After receiving the ransom, the attacker restored access to the files but issued an additional demand: if the company wanted to prevent the stolen R&D data from being publicly leaked, they would have to pay another ransom.

Thus, the company faced a double extortion attack, one ransom to decrypt the files and another to prevent data leakage.

Threat Actor Type:

- Advanced Persistent Threat (APT)
- A highly skilled group, often sponsored by a nation-state.
- Conducts targeted attacks aimed at maintaining long-term access and stealing data.
- Utilizes phishing, zero-day malware, and lateral movement techniques.

Tactics and Techniques:

In this scenario, the attacker sends the victim a fake job offer email containing a malicious macro-enabled PDF. When the engineer opens the PDF, it triggers the execution of the macro. The macro contains malicious PowerShell code that exploits a local vulnerability to obtain system-level privileges. This attack bypasses User Account Control (UAC), allowing privileges to be escalated on the Windows system.

Phase	Technique Used	MITRE ATT&CK ID	Description
Initial Access	Spearphishing Attachment	T1566.001	The attacker sends a fake job offer email containing a malicious macro-enabled PDF.
Execution	Malicious File Execution	T1204.002	The engineer opens the PDF, which triggers the execution of the macro.
	Office Application Macro	T1059.005	The macro contains malicious PowerShell code.
Privilege Escalation	Exploitation for Privilege Escalation	T1068	The malicious code exploits a local vulnerability to obtain system-level privileges.
	Bypass User Account Control (UAC)	T1548.002	The attack bypasses User Account Control (UAC) on Windows to escalate privileges.
Lateral Movement	Remote Services	T1021	The attacker moves laterally from the engineer's system to the domain controller and other servers.
Collection	Data from Information Repositories	T1213	The attacker steals important R&D data from the server.
Exfiltration		T1567.002	The attacker exfiltrates the stolen

	Exfiltration to Cloud/Remote Server		data to an external remote server.
Impact	Data Encrypted for Impact	T1486	The attacker deploys ransomware and encrypts data across multiple systems.
	Exfiltration Over Web Services + Extortion	T1486	The attacker threatens to leak the stolen R&D data if additional ransom payments are not received.

Big Enterprise Company Scenario – Detection & Mitigation:

Detection Techniques:

- **SIEM:**
  Set alerts to detect macro-enabled PDFs, privilege escalation attempts, and suspicious PowerShell commands.
- **EDR:**
  Detects attacks such as local vulnerability exploitation and User Account Control (UAC) bypass.

Log Monitoring:

- **Email logs:**
  To check malicious attachments.
- **MS Office logs:**
  To trace macro execution.
- **PowerShell logs:**
  Unusual script activity.
- **System logs:**
  Signs of User Account Control (UAC) bypass.

Mitigation Recommendations:

MITRE ID	Technique	Description
M1042	Disable or Remove Feature or Program	Disable macros by default in Office applications.

M1026	Privileged Account Management	Limit access to admin accounts, and apply just-in-time access rules.
M1054	Software Configuration	Use secure configurations of email and office software.
M1017	User Training	Make employees aware of fake job offers and phishing scams.
M1050	Exploit Protection	Keep systems updated so that non-vulnerabilities cannot be exploited.