CyberTalkWithPatrickEssien "Operation Data Breach"

Background

A medium-sized financial firm has recently fallen victim to a sophisticated cyber attack, leading to unauthorised data access and exfiltration of sensitive customer information. Your team has been brought in to analyze the attack, identify how the attackers could infiltrate the network and recommend measures to mitigate the risk of future breaches. You will use the **MITRE ATT&CK framework** to guide your analysis and response.

Attack Summary

Initial Access: Attackers conducted a spear-phishing campaign targeting employees in the financial department, tricking one into opening a malicious attachment that installed a backdoor on the network.
Execution: Using the backdoor, attackers were able to execute a script that escalated their privileges within the network.
Persistence: To maintain access, attackers used a common yet overlooked method of persistence by creating a new account within the system's administrative group.
Privilege Escalation: Attackers exploited an unpatched vulnerability to gain higher privileges, allowing them to move freely within the network.
Discovery: Before executing their main objective, the attackers conducted internal reconnaissance to identify where customer data was stored.
Lateral Movement: Attackers used a combination of legitimate credentials and exploitation of trust relationships to move laterally within the network, reaching the server containing sensitive customer data.
Collection: The attackers compiled data from various sources into a staging area within the network.
Exfiltration: Finally, attackers encrypted the collected data and exfiltrated it to an external command and control server over several days to avoid detection.

Task

Mapping the Attack: Use the MITRE ATT&CK framework to map out each stage of the attack, identifying the tactics, techniques, and procedures (TTPs) used by the attackers. Provide a detailed analysis of how each step was carried out and link it to the corresponding tactic and technique in the framework.
Detection and Mitigation: For each identified tactic and technique, propose detection strategies and mitigation measures that could have either prevented the attackers from advancing to the next stage or detected their malicious activities early in the attack chain.
Lessons Learned: Reflect on the simulation exercise and discuss what lessons can be learned from this scenario. Highlight any weaknesses in the current cybersecurity posture of the hypothetical firm and recommend improvements.

Deliverables

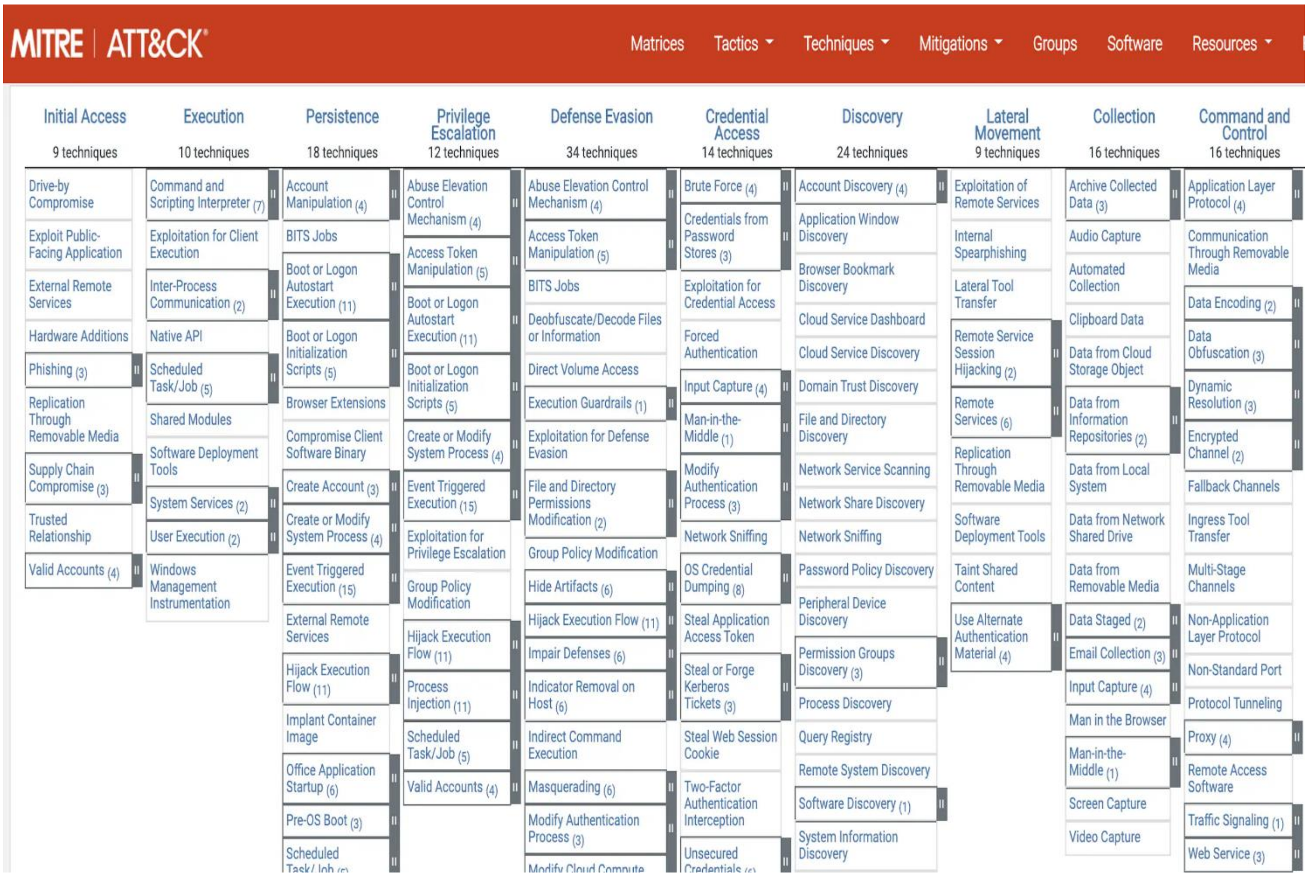
A detailed mapping of the attack using the **MITRE ATT&CK framework.** A set of detection strategies and mitigation measures for each stage of the attack. A presentation or report summarizing the analysis, findings, and recommendations.

BRIEF EXPLANATION OF THE PRESENTATION

Our team used the MITRE ATT&CK methodology as a thorough guide to analyse the assault, identify the attackers' intrusion tactics, and develop effective response plans in response to the sophisticated cyberattack that targeted a medium-sized financial business. The MITRE ATT&CK paradigm gave us a methodical way to classify and comprehend the many phases of the attack lifecycle, which allowed us to precisely map out the tactics, methods, and procedures (TTPs) of the attacker.

We carefully examined every stage of the assault, from gaining access to removing sensitive material, and compared the observed actions to certain methods described in the MITRE ATT&CK architecture. This procedure made it easier to comprehend how the attackers gained access to the network, elevated their privileges, carried out reconnaissance, and carried out their harmful goals. To improve the organization's security posture and lower the chance of future breaches, we also created customized detection tactics and mitigation measures for each strategy and approach that was found. To increase resistance against comparable cyber dangers, these steps included technical controls, procedural improvements, and personnel training programs.

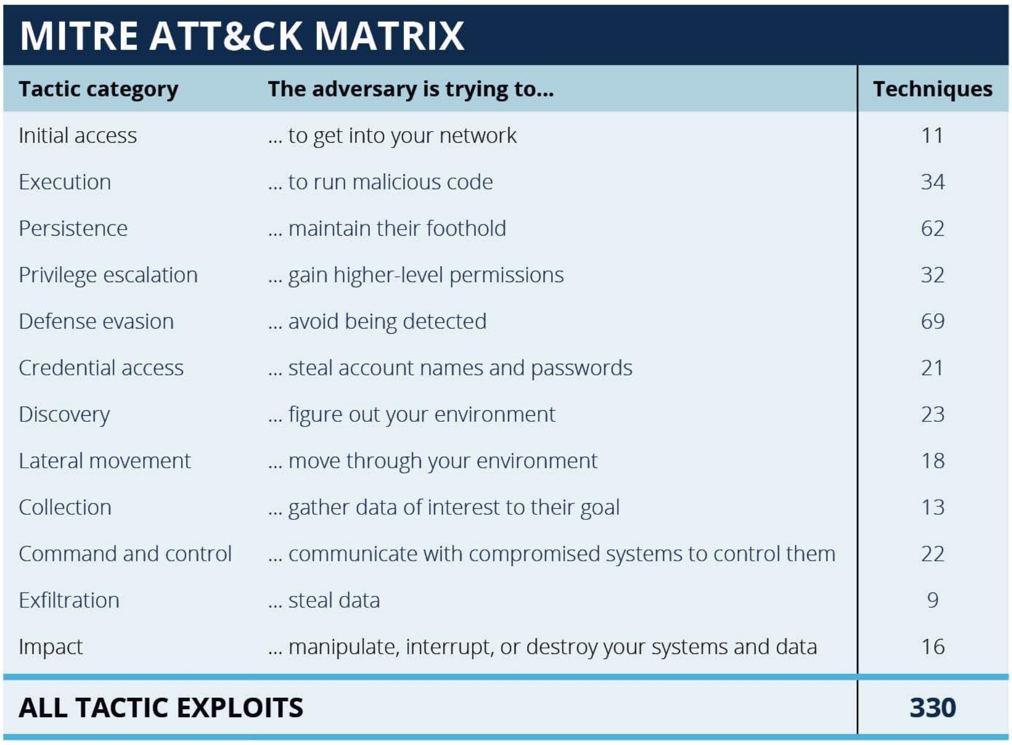
VISUAL REPRESENTATION OF MITRE ATTACK



MITRE | ATT&CK®

Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 24 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Application Layer Protocol
		Hijack Execution Flow (11)	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery		Email Collection (3)	Non-Standard Port
		Implant Container Image	Valid Accounts (4)	Impair Defenses (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling
		Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Proxy (4)
		Pre-OS Boot (3)		Indirect Command Execution	Unsecured Credentials	Process Discovery		Man-in-the-Middle (1)	Remote Access Software
		Scheduled Task/Job (5)		Masquerading (6)		Query Registry		Screen Capture	Traffic Signaling (1)
				Modify Authentication Process (3)		Remote System Discovery		Video Capture	Web Service (3)
				Modify Cloud Compute		Software Discovery (1)			
						System Information Discovery			

PS: Every tactic and technique mentioned in this scenario are all listed on this mitre att&ck image. You can also access each technique using the links next to the IDs.



MITRE ATT&CK MATRIX

Tactic category	The adversary is trying to…	Techniques
Initial access	… to get into your network	11
Execution	… to run malicious code	34
Persistence	… maintain their foothold	62
Privilege escalation	… gain higher-level permissions	32
Defense evasion	… avoid being detected	69
Credential access	… steal account names and passwords	21
Discovery	… figure out your environment	23
Lateral movement	… move through your environment	18
Collection	… gather data of interest to their goal	13
Command and control	… communicate with compromised systems to control them	22
Exfiltration	… steal data	9
Impact	… manipulate, interrupt, or destroy your systems and data	16
ALL TACTIC EXPLOITS		**330**

SOLUTION (Operation Data Breach)

Mapping the Attack:

Use the MITRE ATT&CK framework to map out each stage of the attack, identifying the tactics, techniques, and procedures (TTPs) used by the attackers. Provide a detailed analysis of how each step was carried out and link it to the corresponding tactic and technique in the framework.

- **Attack Stage1: Initial Access**

Tactic: Initial Access

Technique: Spear-phishing Attachment (T1566/001) (https://attack.mitre.org/techniques/T1566/001/)

Description: The attackers conducted a spear-phishing campaign targeting employees in the financial department. One employee opened a malicious attachment, which installed a backdoor on the network.

Detailed Explanation: Spear-phishing involves sending highly targeted emails to specific individuals within an organization, often using social engineering techniques to trick them into opening malicious attachments or clicking on malicious links. In this case, one employee fell victim to the phishing email and opened a malicious attachment, which served as the initial entry point for the attackers.

Spear Phishing Explained
Spear phishing is a targeted cyberattack toward an individual or organization with the end goal of receiving confidential information for fraudulent purposes.
1.
A cybercriminal identifies a piece of data they want and identifies an individual who has it.
2.
The cybercriminal researches the individual and poses as one of their trusted sources.
3.
The cybercriminal convinces their victim to share the data and uses it to commit a malicious act.

Detection Strategy: Implement email security solutions that can detect and block suspicious attachments or links in phishing emails. Train employees on how to recognize and report phishing attempts.

Mitigation Measures: Regularly update and patch software to mitigate known vulnerabilities that could be exploited through malicious attachments. Implement endpoint protection solutions that can detect and block malicious activities initiated by email attachments.

- **Attack Stage 2: Execution**

Tactic: Execution

Technique: Command and Scripting Interpreter (T1059) (https://attack.mitre.org/techniques/T1059/)

Description: Attackers executed a script using the backdoor, allowing them to escalate privileges within the network.

Detailed Explanation: Execution is a tactic that describes techniques used by attackers to run malicious code on a victim's system. This tactic covers various methods attackers employ to execute their payloads, gain control over the victim's environment, and achieve their objectives.

Upon opening the malicious attachment, a script was executed, which installed a backdoor on the network.

Scripting involves the use of scripts or code to automate tasks or perform specific actions on a system. In this attack, the script served as the mechanism for installing the backdoor, allowing the attackers to gain unauthorized access to the network.

Detection Strategy: Monitor for suspicious scripting activity on endpoints or network traffic. Implement behaviour-based detection mechanisms to identify abnormal scripting behaviour indicative of malicious activity.

Mitigation Measures: Restrict execution permissions for scripts and implement application whitelisting to prevent unauthorized execution of scripts. Regularly update and patch software to address vulnerabilities that could be exploited through scripting.

- **Attack Stage 3: Persistence**

Tactic: Persistence

Technique: Create Account (T1136/001) (https://attack.mitre.org/techniques/T1136/001/)

Description: The attackers created a new account within the system's administrative group to maintain access to the network.

Detailed Explanation: Persistence is a tactic used by attackers to maintain access to a compromised system across system reboots, logouts, and other disruptions. It involves techniques employed by adversaries to ensure continued access to the victim's environment, allowing them to maintain, control and execute further malicious activities over an extended period.

To maintain access to the network, the attackers created a new account within the system's administrative group. Creating a new account with elevated privileges allows the attackers to maintain persistence within the network, even if their initial entry point is discovered and remediated.

Detection Strategy: Monitor for unauthorized account creation activities, especially within privileged groups or administrative accounts. Implement user behaviour analytics (UBA) to detect anomalous user account behaviour indicative of account misuse or compromise.

Mitigation Measures: Implement least privilege access controls to restrict the creation of new accounts with elevated privileges. Regularly review and audit user accounts and privileges to identify and remove unnecessary or unused accounts.

- **Attack Stage 4: Privilege Escalation**

Tactic: Privilege Escalation

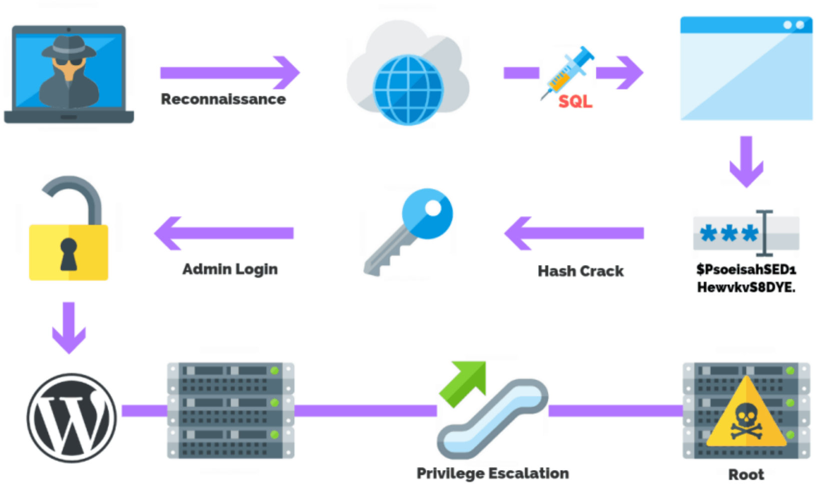
Technique: Exploitation for Privilege Escalation (T1068) (https://attack.mitre.org/techniques/T1068/)

Description: Attackers exploited an unpatched vulnerability to gain higher privileges, enabling them to move freely within the network.

Detailed Explanation: Privilege escalation is a tactic used by adversaries to obtain higher levels of access within a target system or network than they initially had.

After a new account was created, the attackers found and took advantage of a weakness or flaw in the network's defences. In this case, the weakness was the unpatched vulnerability.

A vulnerability is a weakness in a system or software that can be exploited by attackers to gain unauthorized access or perform malicious activities. "Unpatched" means that the vulnerability has not been fixed or addressed by applying a software update or patch provided by the software vendor. In a network, different users have different levels of access or privileges. By exploiting the vulnerability, the attackers were able to gain higher privileges, meaning they obtained access rights beyond what they were initially granted. Once the attackers have gained higher privileges, they can navigate through the network more easily. They can access sensitive information, install malicious software, or carry out other malicious activities without encountering as many obstacles or restrictions.



Detection Strategy: Implement vulnerability scanning and patch management solutions to identify and remediate known vulnerabilities in public-facing applications. Monitor for suspicious activities or anomalous behaviour that could indicate exploitation attempts.

Mitigation Measures: Regularly update and patch software to address known vulnerabilities. Implement network segmentation to limit the impact of successful privilege escalation attempts.

- **Attack Stage 5: Discovery**

Tactic: Discovery

Technique: Browser Information Discovery (Internal Reconnaissance) (T1217) (https://attack.mitre.org/techniques/T1217/)

Description: Before executing their main objective, attackers conducted internal reconnaissance to identify where customer data was stored.

Detailed Explanation: Reconnaissance" refers to the process of gathering information or intelligence about a target before launching an attack. In this case, "internal reconnaissance" means that the attackers were gathering information from within the organization's network.

Before launching the attack to steal or manipulate customer data, attackers need to know where this data is stored within the organization's network. Conducting internal reconnaissance allowed them to gather this crucial information.

By identifying the location of customer data, attackers were able to plan their attacks more effectively. Internal reconnaissance may involve various techniques, such as scanning network infrastructure, probing systems for vulnerabilities, or analyzing network traffic to identify data flows.

Detection Strategy: Monitor for unusual or unauthorized reconnaissance activities, such as excessive querying of network resources or file shares. Implement network and endpoint logging to capture activity indicative of reconnaissance attempts.

Mitigation Measures: Implement access controls and encryption mechanisms to protect sensitive data from unauthorized access. Regularly review and update access permissions to ensure that only authorized personnel have access to sensitive information.

- **Attack Stage 6: Lateral Movement**

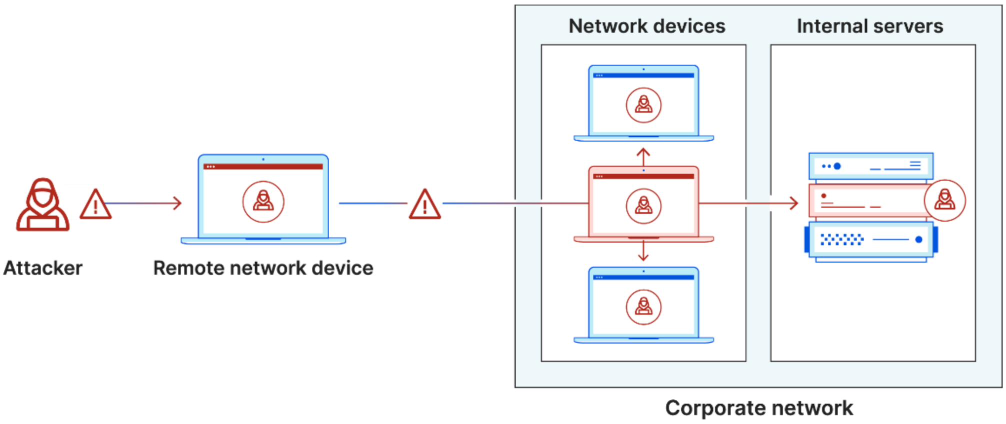
Tactic: Lateral Movement

Technique: Remote Services (T1021) (https://attack.mitre.org/techniques/T1021/)

Description: Attackers used a combination of legitimate credentials and exploitation of trust relationships to move laterally within the network, reaching the server containing sensitive customer data.

Detailed Explanation: Lateral movement is the tactic and technique used by attackers to move within a network, from one system or endpoint to another, to achieve their objectives.

Attackers gain access to the company's computer or system within the network using stolen or compromised credentials (legitimate credentials). After they got in, they used this access to explore and exploit trust relationships between different systems or accounts, which allowed them to move laterally (sideways) across the network. Eventually, they reached the server that holds sensitive customer data, which was their ultimate target.



- **Detection Strategy:** Monitor for unusual or unauthorized lateral movement activities, such as the use of legitimate credentials from unusual locations or systems. Implement network segmentation and access controls to limit lateral movement between network segments.
- **Mitigation Measures:** Implement strong authentication mechanisms, such as multi-factor authentication (MFA), to prevent unauthorized access using stolen or compromised credentials. Regularly review and update trust relationships between systems to minimize the risk of lateral movement.

- **Attack Stage 7: Collection**

Tactic: Collection

Technique: Data from Local System (T1005) (https://attack.mitre.org/techniques/T1005/)

Description: Attackers compiled data from various sources into a staging area within the network.

Detailed Explanation: Attackers gathered data from different sources within the network. These sources could include databases, file shares, user directories, or any other repositories where valuable data is stored. Then, they created a staging area within the network. A staging area is a designated space or location where data is temporarily stored or processed before being moved or utilized for a specific purpose. In this context, the staging area served as a centralized location within the network where the attackers could consolidate and organize the data they had collected.

Detection Strategy: Collection is the tactic used by attackers to gather or consolidate data from various sources within the compromised network. Monitor for unusual or unauthorized data access activities, such as large-scale data transfers or access to sensitive files or databases. Implement data loss prevention (DLP) solutions to prevent unauthorized data exfiltration.

Mitigation Measures: Implement encryption mechanisms to protect sensitive data at rest and in transit. Implement data classification and tagging to identify and protect sensitive data from unauthorized access or exfiltration.

- **Attack Stage 8: Exfiltration**

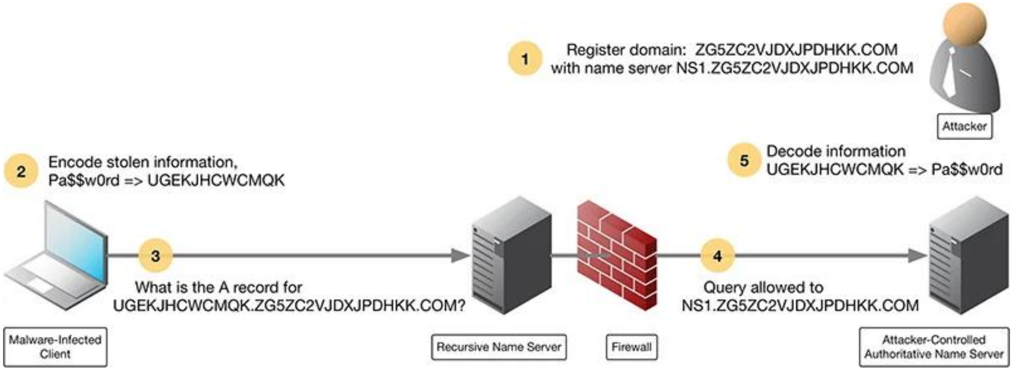
Tactic: Exfiltration

Technique: Exfiltration Over C2 Channel (T1041) (https://attack.mitre.org/techniques/T1041/)

Description: Attackers encrypted the collected data and exfiltrated it to an external command and control server over a period of several days to avoid detection.

Detailed Explanation: Exfiltration means the unauthorized transfer of data from a victim's network to an external location controlled by the attackers. It is one of the stages in the cyber attack lifecycle where attackers steal sensitive information or data and remove it from the compromised network for malicious purposes, such as espionage, intellectual property theft, or financial gain.

After compiling data from various sources, the attackers took the information they found on the compromised network and turned it into a secret code that only they could understand. This makes it harder for anyone else to see what the information is if they manage to intercept it. The attackers sent the encrypted information to another computer outside of the compromised network. This other computer is controlled by the attackers and is used to receive and store the stolen information. Instead of sending all the stolen information at once, the attackers sent it in small amounts over several days. This makes it less likely for anyone monitoring the network to notice anything suspicious since the amount of information left each day is small.



Detection Strategy: Monitor for unusual or unauthorized data exfiltration activities, such as large volumes of data leaving the network or connections to suspicious external IP addresses. Implement network traffic analysis and anomaly detection solutions to detect and block suspicious exfiltration attempts.

Mitigation Measures: Implement data loss prevention (DLP) solutions to prevent unauthorized data exfiltration. Implement network segmentation to limit communication between internal systems and external command and control servers.

Lessons Learned:

- The importance of employee training and awareness in recognising and avoiding phishing attacks.
- The critical need for timely patching and updating of systems to prevent exploitation of vulnerabilities.
- The significance of implementing defence-in-depth security controls, including email security, endpoint protection, and network monitoring, to detect and respond to threats at various stages of the attack chain.
- The need for proactive measures, such as regular security assessments and penetration testing, to identify and remediate security weaknesses before they can be exploited by attackers.