Document Reference:	IURTU-1	Effective Date:	10 May 2024
Document Name:	Improper Usage Red Team Usecase	Expiry Date:	10 May 2025

Improper Usage Red Team Usecases

Redback Operations

Document Owner:	Purple team	Last Modified By:	Liya Thomas
Next Review Date:	17 July 2024	Last Modified on:	10 May 2024

Version	Modified By	Approver	Date	Changes made
0.1	Liya Thomas		10 May 2024	First Draft

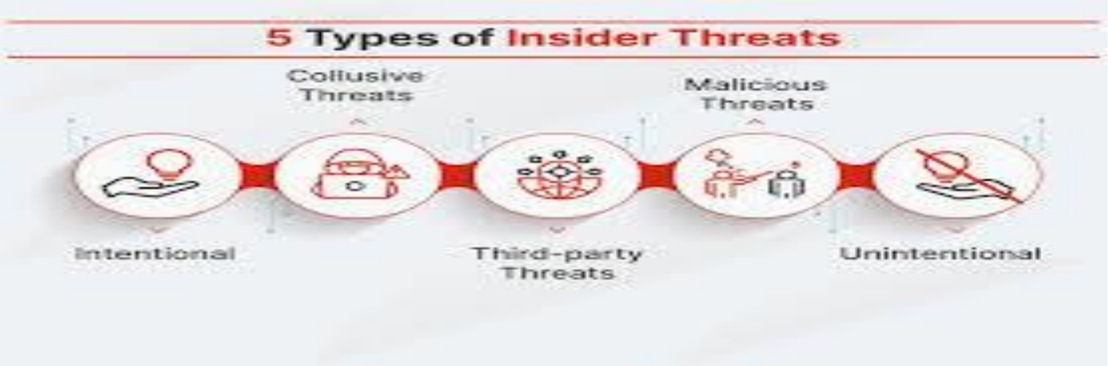
Table of Contents

1 Introduction:

In today's dynamic cybersecurity landscape, organizations face a myriad of threats, ranging from insider attacks to external breaches and everything in between. To effectively combat these threats, organizations must proactively assess their security posture and identify vulnerabilities before adversaries exploit them. Red team exercises play a crucial role in this regard, allowing organizations to simulate real-world attack scenarios and test the effectiveness of their defenses.

This document outlines various red team playbooks focusing on insider threats, external attacks, data breaches, phishing incidents, ransomware attacks, and credential theft. Each playbook provides a comprehensive overview of the objectives, steps involved, and tools and techniques utilized to simulate these specific threat scenarios within Redback Operations.

2 Insider Threat



2.1 Objective: Gain Elevated Privileges

The primary objective of a red team exercise focusing on insider threats within Redback Operations is to simulate how an adversary could gain elevated privileges within the organization's systems to access sensitive data or carry out malicious activities without detection. By achieving this objective, the red team aims to highlight vulnerabilities in access controls, trust relationships, and security mechanisms, enabling the organization to implement effective countermeasures and mitigate the risk of insider threats effectively.

2.2 Steps in Simulating Insider Threats

1. Identify Vulnerable or Disgruntled Employees: The first step in the red team exercise is to identify employees within Redback Operations who may pose a threat due to their access to

sensitive systems or data. This involves conducting thorough reconnaissance to pinpoint individuals with access privileges that could be exploited for malicious purposes. Vulnerable or disgruntled employees are particularly targeted as they may be more susceptible to manipulation or coercion.

2. Exploit Weaknesses in Access Control Mechanisms: Once potential insider threats are identified, the red team will seek to exploit weaknesses in access control mechanisms or misconfigurations to gain initial access to the organization's systems. This could involve exploiting vulnerabilities in authentication protocols, weak passwords, or insecure configurations to bypass security controls and establish a foothold within the network.

3. Use Social Engineering Tactics or Insider Knowledge: Social engineering plays a crucial role in escalating privileges and bypassing security controls in insider threat scenarios. Red teamers may deploy phishing emails, pretexting, or baiting techniques to manipulate insiders into divulging credentials, providing access to sensitive systems, or executing malicious payloads. Alternatively, insider knowledge obtained through reconnaissance may be leveraged to gain trust and access to critical assets.

2.3 Tools and Techniques for Insider Threat Simulations

1. Social Engineering: Phishing kits, pretexting scripts, and social engineering toolkits can be used to craft convincing phishing emails or pretexting scenarios tailored to exploit the psychological vulnerabilities of targeted insiders.

2. Exploitation of Trust Relationships: Tools such as BloodHound or Rubeus can be employed to map trust relationships within the organization and identify paths to privileged accounts or sensitive data accessible to insiders.

3. Exploitation of Misconfigurations: Vulnerability scanners and penetration testing tools can help identify misconfigured permissions or access control lists (ACLs) that could be exploited by insiders to escalate privileges and gain unauthorized access to critical assets.

3 External Attack

External Suppliers
Poor Defence
Outdated Software
WHAT ARE EXTERNAL THREATS?
Cyber Attack
Exploitation
Social Engineering

3.1 Objective: Compromise External-Facing Systems

The primary objective of a red team exercise focusing on external attacks within Redback Operations is to simulate how adversaries could compromise the organization's systems or networks from external sources to gain elevated privileges and access sensitive data. By achieving this objective, the red team aims to identify vulnerabilities in external-facing systems, assess the effectiveness of existing defenses, and recommend improvements to mitigate the risk of external attacks effectively.

3.2 Steps

1. Identify Vulnerabilities in External-Facing Systems: The first step in the red team exercise is to identify vulnerabilities in Redback Operations' external-facing systems or network infrastructure. This involves conducting comprehensive vulnerability assessments and penetration testing to identify potential entry points and weaknesses that could be exploited by attackers to gain unauthorized access.

2. Exploit Vulnerabilities to Gain Initial Access: Once vulnerabilities are identified, the red team will seek to exploit them to gain initial access or establish footholds within the organization's network. This may involve exploiting known vulnerabilities in software, misconfigured network services, or weak authentication mechanisms to bypass security controls and gain a foothold on the network.

3. Escalate Privileges: With initial access established, the red team will aim to escalate privileges to gain administrative or superuser access for deeper penetration into Redback Operations' systems. This may involve exploiting vulnerabilities in privilege escalation mechanisms, weakly protected accounts, or misconfigured access controls to gain higher levels of access and control over the network.

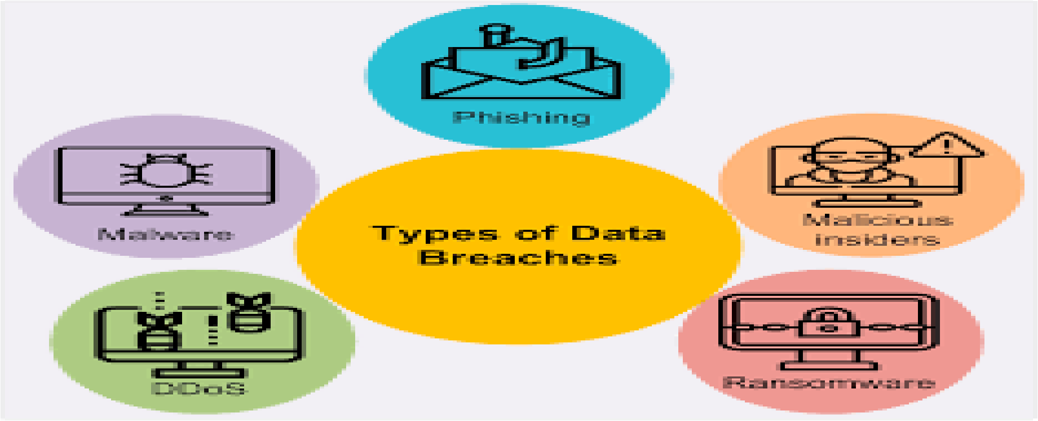
3.3 Tools and Techniques

1. Vulnerability Scanners: Tools like Nessus and OpenVAS can be used to conduct automated vulnerability scans of Redback Operations' external-facing systems, identifying potential vulnerabilities that could be exploited by attackers.

2. Exploit Frameworks: Metasploit and Exploit-DB provide a comprehensive database of known exploits and payloads that can be used to exploit vulnerabilities identified during the scanning phase, gaining unauthorized access to target systems.

3. Privilege Escalation Exploits: Tools like Windows-Exploit-Suggester and Linux Exploit Suggester can be used to identify and exploit vulnerabilities that allow attackers to escalate privileges and gain administrative access to target systems.

4 Data Breaches



4.1 Objective: Obtain Elevated Privileges and Exfiltrate Data

The primary objective of a red team exercise focusing on data breaches within Redback Operations is to simulate how adversaries could obtain elevated privileges to access and exfiltrate sensitive data from the organization's systems or databases. By achieving this objective, the red team aims to identify weaknesses in data storage and access controls, exploit vulnerabilities or misconfigurations to gain unauthorized access, and exfiltrate sensitive data without detection.

4.2 Steps

1. Identify Weaknesses in Data Storage and Access Controls: The first step in the red team exercise is to identify weaknesses in data storage or access controls that could allow unauthorized access to sensitive data. This involves conducting thorough assessments of the organization's data storage mechanisms, databases, file repositories, and access control policies to identify potential entry points for attackers.

2. Exploit Vulnerabilities or Misconfigurations: Once weaknesses are identified, the red team will seek to exploit vulnerabilities or misconfigurations to gain access to databases or file repositories containing sensitive data. This may involve exploiting unpatched vulnerabilities, misconfigured permissions, or weak authentication mechanisms to bypass security controls and gain unauthorized access to the target systems.

3. Escalate Privileges: With access to the target systems obtained, the red team will aim to escalate privileges to gain access to restricted or confidential data. This may involve exploiting vulnerabilities in privilege escalation mechanisms, weakly protected accounts, or misconfigured access controls to gain higher levels of access and retrieve sensitive data stored within the organization's databases.

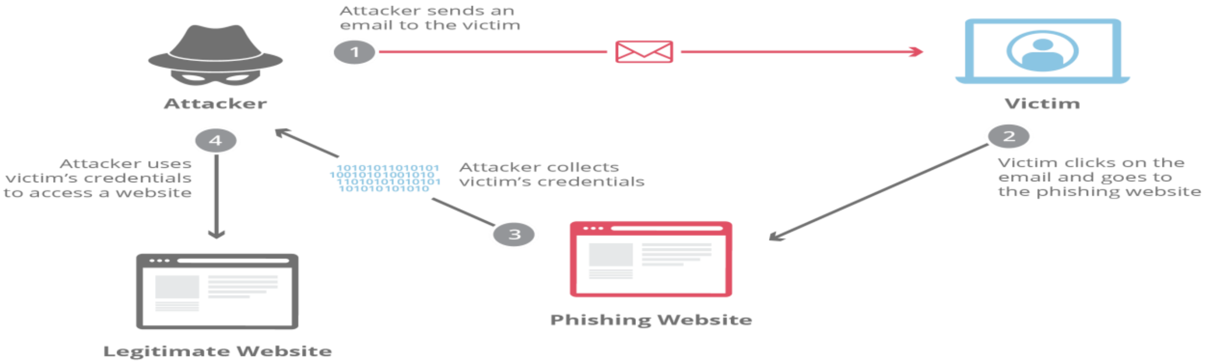
4.3 Tools and Techniques

1. Exploitation of Unpatched Vulnerabilities: Techniques like SQL Injection can be used to exploit vulnerabilities in web applications or database management systems, allowing attackers to manipulate SQL queries and gain unauthorized access to databases.

2. SQL Injection Tools: Tools like SQLMap and Burp Suite automate the process of identifying and exploiting SQL injection vulnerabilities, enabling attackers to retrieve sensitive data from databases without requiring extensive manual intervention.

3. Data Exfiltration Tools: Tools like Mimikatz and BloodHound can be used to extract sensitive data from compromised systems and exfiltrate it to external servers or storage locations, bypassing security controls and evading detection.

5 Phishing Incident


Attacker sends an email to the victim
1
Attacker
Victim
4
Attacker uses victim's credentials to access a website
10101011010101 10010101001010 11010101010101 101010101010
Attacker collects victim's credentials
2
Victim clicks on the email and goes to the phishing website
3
Phishing Website
Legitimate Website

5.1 Objective: Gain Elevated Privileges through Social Engineering

The primary objective of a red team exercise focusing on phishing incidents within Redback Operations is to demonstrate how adversaries can gain elevated privileges by tricking employees into divulging their credentials or providing access to sensitive systems. By achieving this objective, the red team aims to assess the effectiveness of the organization's phishing awareness training programs, identify vulnerable employees, and highlight the importance of implementing robust security measures to prevent phishing attacks.

5.2 Steps

1. Craft Convincing Phishing Emails: The first step in the red team exercise is to craft convincing phishing emails or messages impersonating trusted sources within Redback Operations. These emails may appear legitimate and include enticing subject lines or urgent requests to prompt recipients to take action, such as clicking on malicious links or providing login credentials.

2. Distribute Phishing Emails to Targeted Employees: Once the phishing emails are crafted, the red team will distribute them to targeted employees and stakeholders within the organization. These targeted individuals may include employees with access to sensitive systems or data, executives, or individuals in positions of authority who are more likely to be targeted by adversaries.

3. Exploit Compromised Credentials: Upon successful phishing attempts, the red team will exploit compromised credentials to escalate privileges and access sensitive data or systems within Redback Operations. This may involve using keylogging or form grabbing techniques to capture login credentials entered by unsuspecting employees, bypassing multi-factor authentication (MFA), or exploiting trust relationships to gain access to privileged accounts.

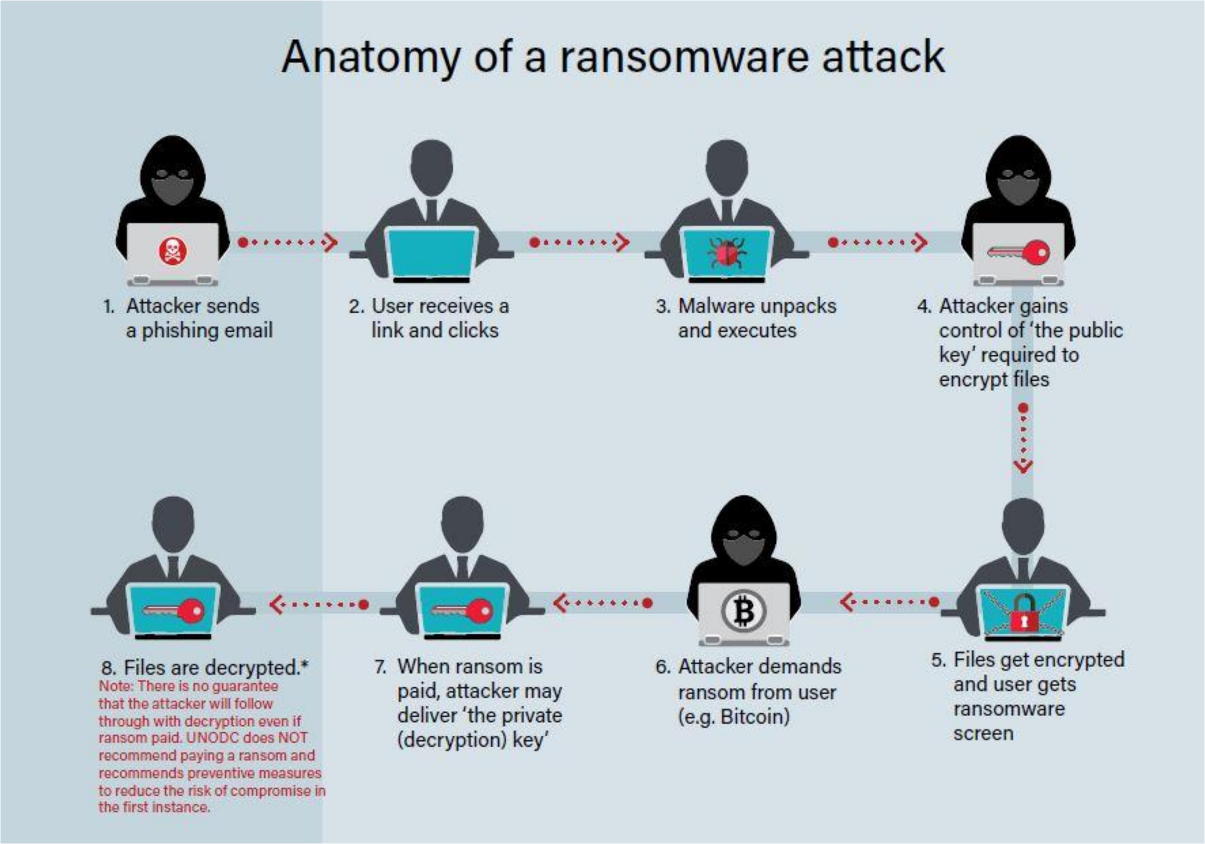
5.3 Tools and Techniques

1. Phishing Frameworks: Tools like GoPhish and PhishingFrenzy automate the process of crafting and distributing phishing emails, enabling attackers to simulate real-world phishing attacks efficiently.

2. Credential Harvesting: Techniques such as keylogging and form grabbing can be used to capture login credentials entered by targeted individuals, allowing attackers to gain unauthorized access to sensitive systems or data.

3. 2FA Bypass Techniques: Social engineering tactics or phishing of 2FA tokens can be employed to bypass multi-factor authentication measures and gain access to compromised accounts or systems.

6 Ransomware


Anatomy of a ransomware attack
1. Attacker sends a phishing email
2. User receives a link and clicks
3. Malware unpacks and executes
4. Attacker gains control of 'the public key' required to encrypt files
5. Files get encrypted and user gets ransomware screen
6. Attacker demands ransom from user (e.g. Bitcoin)
7. When ransom is paid, attacker may deliver 'the private (decryption) key'
8. Files are decrypted.*
Note: There is no guarantee that the attacker will follow through with decryption even if ransom paid. UNODC does NOT recommend paying a ransom and recommends preventive measures to reduce the risk of compromise in the first instance.

6.1 Objective: Deploy Ransomware to Encrypt Data

The primary objective of a red team exercise focusing on ransomware attacks within Redback Operations is to demonstrate how adversaries can gain elevated privileges to deploy ransomware within the organization's systems or networks. By achieving this objective, the red team aims to assess the effectiveness of the organization's security controls, identify vulnerabilities or misconfigurations that may lead to ransomware attacks, and highlight the importance of implementing proactive security measures to mitigate the risk of such incidents.

6.2 Steps

1. Identify Vulnerabilities or Misconfigurations: The first step in the red team exercise is to identify vulnerabilities or misconfigurations in Redback's systems that may allow for unauthorized access or execution of malicious code. These vulnerabilities could include

unpatched software, weak authentication mechanisms, or misconfigured access controls that adversaries can exploit to gain initial access to the organization's network.

2. Exploit Vulnerabilities to Gain Initial Access: Once vulnerabilities are identified, the red team will exploit them to gain initial access to Redback's systems or networks. This may involve delivering malware through phishing emails, exploiting known vulnerabilities using exploit kits, or leveraging compromised credentials obtained through previous reconnaissance activities.

3. Escalate Privileges for Deploying Ransomware: After gaining initial access, the red team will escalate privileges to gain administrative access within Redback's network. This step is crucial for deploying ransomware payloads effectively and ensuring that adversaries have sufficient access to encrypt critical data and systems. Privilege escalation exploits, such as known vulnerabilities or custom exploits, may be used to escalate privileges and gain administrative access.

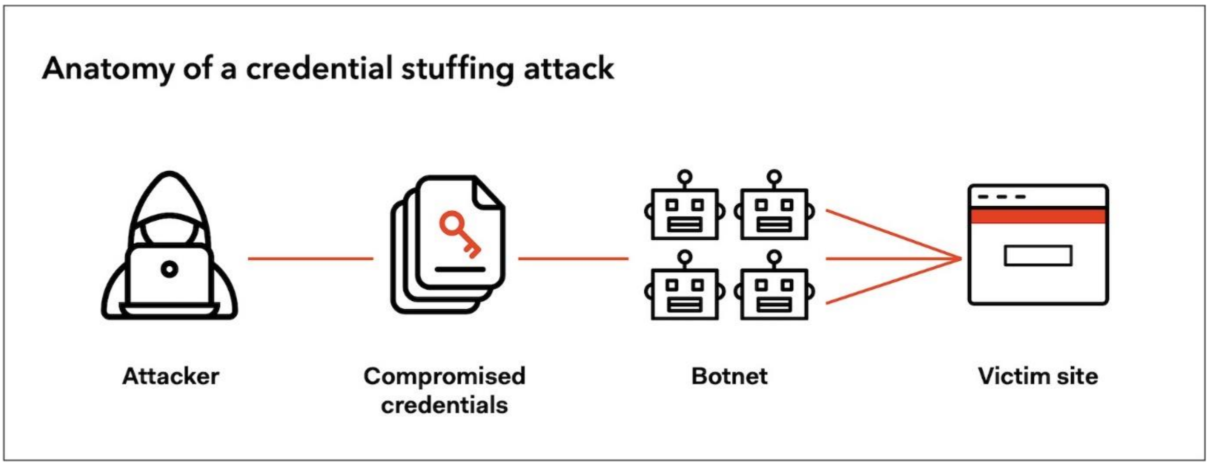
6.3 Tools and Techniques for Ransomware Attacks

1. Malware Delivery: Phishing emails and exploit kits are commonly used to deliver ransomware payloads to targeted systems or networks, exploiting vulnerabilities or enticing users to click on malicious links or attachments.

2. Lateral Movement: Adversaries may use compromised credentials obtained through phishing or exploitation of trust relationships to move laterally within the network, gaining access to additional systems or resources.

3. Privilege Escalation Exploits: Known vulnerabilities or custom exploits can be used to escalate privileges and gain administrative access within Redback's network, enabling adversaries to deploy ransomware payloads effectively.

7 Credential Theft



7.1 Objective: Obtain Elevated Privileges via Credential Theft

The primary objective of simulating credential theft attacks within Redback Operations is to demonstrate how adversaries can obtain elevated privileges within the organization's systems or networks by stealing credentials from employees or stakeholders. By achieving this objective, the red team aims to assess the effectiveness of the organization's authentication mechanisms, identify vulnerabilities in its security posture, and highlight the importance of implementing robust measures to prevent unauthorized credential access.

7.2 Steps

1. Identify Employees or Stakeholders with Privileged Access: The initial step in the red team exercise is to identify employees or stakeholders within Redback Operations who have privileged access to critical systems or data. This may involve conducting reconnaissance activities to gather information about user roles, responsibilities, and access privileges within the organization.

2. Use Phishing Attacks or Social Engineering Tactics: Once high-privileged users are identified, the red team will employ phishing attacks, social engineering tactics, or other techniques to trick users into revealing their login credentials or authentication tokens. This may include sending phishing emails impersonating trusted sources or creating fake login pages to harvest credentials.

3. Escalate Privileges Using Compromised Credentials: After obtaining credentials from targeted users, the red team will escalate privileges within Redback's systems or networks to gain access to sensitive data or carry out unauthorized activities. This step may involve

using compromised credentials to bypass authentication mechanisms, access restricted resources, or impersonate legitimate users to evade detection.

7.3 Tools and Techniques

1. Credential Phishing: Phishing emails and phishing websites are commonly used to trick users into divulging their login credentials by impersonating trusted entities or enticing users to click on malicious links.

2. Keylogging: Malware or keyloggers can be used to capture keystrokes entered by users, allowing adversaries to record login credentials and authentication tokens without the user's knowledge.

3. Pass-the-Hash: Credential theft tools and techniques such as pass-the-hash attacks involve exploiting hashed credentials stored on compromised systems to authenticate to other systems within the network, bypassing the need for plaintext passwords.

8 Conclusion

In conclusion, red team exercises serve as invaluable tools for organizations to enhance their cybersecurity resilience by identifying and addressing weaknesses in their defenses. By simulating realistic attack scenarios, organizations can better understand their adversaries' tactics, techniques, and procedures, allowing them to bolster their security measures and mitigate the risk of cyber threats effectively.

Through the outlined playbooks, Redback Operations can gain insights into potential vulnerabilities within their systems and networks, assess the effectiveness of existing security controls, and develop proactive strategies to strengthen their overall security posture. By investing in red team exercises and adopting a proactive approach to cybersecurity, organizations can stay one step ahead of adversaries and safeguard their critical assets against evolving threats.

9 References

insider threat - https://www.fortinet.com/content/fortinet-com/en_us/resources/cyberglossary/insider-threats/_jcr_content/par/c05_container_copy_c/par/c28_image.img.jpg/1662063544973.jpg

External attack - https://securetriad.io/wp-content/uploads/2021/06/What-are-External-Threats-1024x640.png

data breaches - https://www.researchgate.net/publication/376981653/figure/fig1/AS:11431281215077478@1703948451371/Types-of-data-breach-attacks-Types-of-data-breach-attacks.png

Phishing Incident - https://www.cloudflare.com/img/learning/security/threats/phishing-attack/diagram-phishing-attack.png

Ransomware attack - https://www.unodc.org/roseap/uploads/images/2021/10/cybercrime/ransom_2.jpg

Credential Theft attack- https://images.ctfassets.net/23aumh6u8s0i/ohyMA4nbwQgkGF77RnSOs/b8997e017022790f156a985fb97c375d/anatomy-credential-stuffing.jpg