Ransomware Attack

I. Introduction

A **ransomware attack** is a type of malicious cyberattack where an attacker encrypts a victim's data or locks them out of their system, then demands payment (typically in cryptocurrency) in exchange for restoring access. The victim may be an individual, a corporation, a government organization, or even a healthcare provider. The attack typically spreads via phishing emails, malicious attachments, or exploiting software vulnerabilities.

II. Key Characteristics of a Ransomware Attack

1. **Encryption of Files**: Ransomware often encrypts files on the infected system, rendering them unreadable to the victim. A ransom note typically appears on the screen, demanding payment in exchange for the decryption key.
2. **Locking Systems or Devices**: In some cases, ransomware may lock the victim's device, preventing access to the operating system, applications, or files. The victim is presented with a message demanding payment to unlock the system.
3. **Demand for Ransom**: The attacker demands payment, often in cryptocurrency like Bitcoin or Monero, to provide the decryption key or to unlock the device. The ransom can range from hundreds to millions of dollars, depending on the scale of the attack.
4. **Threats of Data Deletion or Exposure**: Some ransomware groups threaten to delete the encrypted data or leak it publicly if the ransom isn't paid. The ransom note may contain instructions on how to make the payment, and it usually includes a deadline.

III. Types of Ransomwares

1. **Crypto Ransomware**: This is the most common form of ransomware. It encrypts the victim's files using strong encryption algorithms, making them inaccessible. Examples include:
    - **WannaCry**: One of the most notorious ransomware attacks, WannaCry spread in 2017, exploiting vulnerabilities in Windows systems (specifically the SMB protocol). It infected hundreds of thousands of computers worldwide, locking them and demanding Bitcoin for decryption.
    - **NotPetya**: A similar attack to WannaCry but with the primary aim of destruction, NotPetya spread quickly and hit major organizations in Ukraine before infecting systems worldwide.
2. **Locker Ransomware**: This type of ransomware locks the victim out of their device, preventing access to the operating system or applications but not necessarily encrypting files. The attacker demands payment to unlock the system.

- **Winlocker**: A well-known example of locker ransomware that locks the victim's screen and displays a message demanding a ransom to unlock it.

3. **Scareware**: Scareware doesn't directly encrypt or lock files but displays fake alerts or warnings, often claiming the system is infected with malware or needs to be "cleaned." The victim is tricked into paying for a bogus anti-virus or cleaning tool.
    - **FauxFix**: A common scareware tactic that mimics legitimate security tools and claims the system is infected, leading users to pay for unnecessary software.
4. **Doxware (or Leakware)**: This variation involves the threat of publicly releasing sensitive information, such as personal, financial, or business data, unless the victim pays the ransom.
    - **Sodinokibi (REvil)**: This ransomware variant is known for encrypting files and threatening to leak sensitive data online if the ransom is not paid. It targets high-profile organizations and extorts significant amounts of money.

IV. Tools used by attackers to perform Brute Force attack

Attackers utilize various tools at different stages of a ransomware attack to achieve their objectives, from gaining initial access to delivering the ransomware payload and encrypting data. These tools often include legitimate software abused for malicious purposes or custom-built malware. Here's an overview of the most commonly used tools for ransomware attacks:

1. Tools for Initial Access: Attackers use tools and methods to infiltrate systems and gain unauthorized access.

- Phishing Tools: GoPhish, PhishMe, Emotet and QakBot
- Exploitation Frameworks: Metasploit Framework, Cobalt Strike.
- Credential Harvesting Tools: Mimikatz, LaZagne
- Brute-Force and Dictionary Tools: Hydra, Medusa, SQLmap

2. Tools for Lateral Movement: Once inside a network, attackers use these tools to move laterally and identify high-value targets.

- Remote Administration Tools (RATs): TeamViewer, AnyDesk, NanoCore, njRAT
- Windows Admin Tools: PsExec, WMIC
- Privilege Escalation Tools: BloodHound, PowerSploit

3. Tools for Reconnaissance: Attackers gather information about the network and connected devices to identify potential targets.

- Network Scanners: Nmap, Advanced IP Scanner
- System Discovery Tools: SharpHound
- Packet Sniffers: Wireshark

4. Tools for Ransomware Deployment: Once the attackers have identified the targets, they use these tools to deliver the ransomware payload.

- Malware Builders and Droppers: Ransomware-as-a-Service, MSFVenom
- Custom Scripts: PowerShell Scripts, Batch Scripts (.bat)
- Exploit Kits: EternalBlue (used in WannaCry), Angler Exploit Kit

5. Tools for Data Exfiltration: Before encrypting data, attackers may steal sensitive information for double extortion tactics.

- File Transfer Tools: Rclone, WinSCP
- Archiving Tools: WinRAR, 7-Zip
- Command-Line Tools: curl, wget

6. Tools for Data Encryption: These tools are specifically designed to encrypt files and hold them for ransom.

- Ransomware Families: LockBit, REvil, Conti, Ryuk, Cerber, Maze
- Backup Destruction: Ransomware often deletes or disables backups to ensure victims cannot recover files without paying.
- Shadow Copy Management Tools: vssadmin.exe, wbadmin.exe
- Disk Wiping Tools: SDelete, DBAN

V. Examples of Famous Ransomware Attacks

1. WannaCry (2017)

- **Method of Attack**: WannaCry exploited a vulnerability in Windows operating systems known as **EternalBlue**, which was leaked from the NSA (National Security Agency). The ransomware propagated by scanning for unpatched systems over the network.
- **Impact**: It affected over 200,000 computers in more than 150 countries, including hospitals, governments, and businesses.
- **Outcome**: While some organizations paid the ransom, the attack caused significant damage to critical infrastructure, particularly in the UK's National Health Service (NHS).

2. NotPetya (2017)

- **Method of Attack**: Like WannaCry, NotPetya exploited the EternalBlue vulnerability but also spread through software updates from a Ukrainian accounting software company.
- **Impact**: It targeted systems in Ukraine and spread to other countries, disrupting businesses and causing financial losses exceeding $10 billion.
- **Outcome**: While the ransom note was present, NotPetya's primary objective appeared to be the destruction of data, not profit.

3. REvil (Sodinokibi) (2020-2021)

- **Method of Attack**: REvil ransomware used phishing emails, vulnerabilities in managed service providers (MSPs), and other exploits to gain access to networks.
- **Impact**: It targeted high-profile companies, including JBS Foods and Kaseya. In the Kaseya attack, REvil affected more than 1,500 businesses worldwide.
- **Outcome**: The attackers demanded millions of dollars in ransom. U.S. authorities eventually launched efforts to dismantle REvil's infrastructure in late 2021.

4. Colonial Pipeline (2021)

- **Method of Attack**: The Colonial Pipeline attack involved a ransomware attack by the DarkSide group. The attackers accessed the company's network through a compromised VPN account.
- **Impact**: The attack disrupted fuel supply across the eastern U.S., causing fuel shortages and panic buying.
- **Outcome**: Colonial Pipeline paid a ransom of $4.4 million, although the U.S. authorities later managed to recover a portion of the payment.

VI. How ransomware Attack Works

A ransomware attack is a type of cyberattack in which attackers infect a target's system with malware that encrypts data or locks access to critical systems until a ransom is paid. Below is a step-by-step breakdown of how ransomware attacks typically work, including common methods used by attackers to achieve their objectives.

1. Initial Access: How Attackers Infiltrate the System

Attackers first gain access to the target system using one or more of the following methods:

- **Phishing Emails:** Emails containing malicious links or attachments trick victims into clicking and executing the ransomware payload. Example: A PDF file with embedded macros downloads the ransomware when opened.
- **Exploitation of Vulnerabilities:** Attackers exploit unpatched software vulnerabilities (e.g., in operating systems, browsers, or remote desktop protocols). Example: WannaCry used the EternalBlue exploit to target SMBv1 vulnerabilities.
- **Brute Force Attacks:** Weak passwords are cracked through brute force or dictionary attacks, granting attackers access to systems or accounts. Example: Attackers brute-force an RDP login to access internal servers.
- **Malicious Websites or Ads:** Victims are lured into visiting malicious websites or clicking on ads, which trigger ransomware downloads. Example: Drive-by downloads from compromised websites.
- **Trojan Malware:** Ransomware may arrive as part of a Trojan download bundled with other software. Example: An installer for a cracked application includes ransomware.

2. Reconnaissance: Mapping the Target's Network

Once inside the system, attackers perform reconnaissance to gather information about the network.

- **Lateral Movement:** Attackers use tools like **PsExec**, **Mimikatz**, or **Cobalt Strike** to move laterally across the network. They look for high-value targets, such as servers, databases, and backups.
- **Credential Harvesting:** Tools like **Mimikatz** or **LaZagne** are used to extract stored credentials. Attackers escalate privileges to gain administrative control.
- **Network Mapping:** Attackers use tools like **Nmap** or **SharpHound** to identify connected devices, shared drives, and sensitive data.

3. Payload Deployment: Installing Ransomware

Once the attackers have identified key systems, they deploy the ransomware payload.

- **Manual Execution:** Attackers may manually launch the ransomware on critical systems or endpoints. Example: Executing the ransomware payload using **PsExec**.
- **Automated Spread:** Some ransomware, such as **WannaCry** and **NotPetya**, spreads automatically across networks using exploits like EternalBlue.
- **Fileless Techniques:** Ransomware may run in memory using PowerShell scripts to avoid detection. Example: A PowerShell command downloads and executes the ransomware.

4. Encryption: Locking the Victim’s Data

The ransomware encrypts files on the target systems using strong encryption algorithms, making the data inaccessible.

- **Encryption Process:** Files are encrypted using symmetric (AES) or asymmetric (RSA) algorithms. File extensions are often modified (e.g., .encrypted, .lockbit).
- **Targeted Files:** Ransomware typically targets critical data files like documents, spreadsheets, databases, and backups. Example: A folder containing business-critical customer records is encrypted.
- **Backup Destruction:** The ransomware deletes or disables shadow copies and backup systems. Command: vssadmin delete shadows /all /quiet.

5. Ransom Note Delivery: Demanding Payment

After encryption, the ransomware displays a ransom note to the victim.

- **Details in the Note:** Instructions on how to pay the ransom, often in cryptocurrency (e.g., Bitcoin). A unique identifier or decryption key associated with the victim. A warning that data will be permanently deleted if payment isn’t made within a deadline.

- **Communication Channels:** Some ransomware groups provide a dark web portal or email address for victims to negotiate. Example: A Tor-based portal displays the payment instructions.

6. Communication with Command-and-Control (C2) Servers

During or after deployment, ransomware may communicate with the attacker's C2 servers.

- **C2 Server Activities:** Retrieve encryption keys. Send information about the victim's system and encrypted files. Receive commands for further attacks.
- **Evading Detection:** Attackers may use DNS tunneling or Tor for secure, anonymous communication.

7. Double Extortion: Data Exfiltration

In modern ransomware attacks, attackers often steal sensitive data before encrypting files.

- **Data Theft:** Stolen data is used to pressure victims into paying the ransom, even if backups exist. Example: Attackers threaten to release proprietary business data unless the ransom is paid.
- **Proof of Theft:** Attackers may leak samples of stolen data to demonstrate their capability.

8. Propagation: Spreading to Other Systems

Advanced ransomware may propagate to other systems to maximize impact.

- **Network Worm Behavior:** Worm-like ransomware spreads to other devices without user intervention. Example: WannaCry's use of SMB exploits to spread automatically.
- **Targeting High-Value Assets:** Attackers prioritize servers, backups, and other critical infrastructure.

9. Payment and Decryption

Victims must decide whether to pay the ransom or attempt recovery without paying**.**

- **Ransom Payment:** If the ransom is paid, attackers may provide a decryption key (though there's no guarantee). Payment is usually made via Bitcoin or other cryptocurrencies.
- **Decryption Tool:** If provided, the attacker's decryption tool is used to recover the files. Example: A company pays $100,000 in Bitcoin and receives a decryption utility.

VII. List of Incidents in Microsoft Sentinel related to Ransomware Attack

1. Suspicious File Encryption Activities: An unusually high number of files are being encrypted within a short timeframe.

2. Anomalous Process Execution: Execution of processes commonly associated with ransomware (e.g., PowerShell, wmic.exe, vssadmin.exe) or processes exhibiting unusual behaviour.

3. Brute Force or Unauthorized Access Attempts: Ransomware often starts with gaining unauthorized access through brute force attacks, phishing campaigns, or credential theft.

4. Lateral Movement in the Network: Ransomware operators attempt to spread across systems within the network.

5. Anomalous Network Traffic or Data Exfiltration: Detection of unusual outbound traffic that could indicate ransomware communicating with command-and-control (C2) servers or exfiltrating data before encryption.

6. Ransom Note Detection: Detection of ransomware-generated files, such as ransom notes (.txt, .html), in shared directories or endpoints.

7. Disabled Security Features: Ransomware often attempts to disable antivirus, endpoint protection, or security tools.

8. Suspicious Use of Admin Tools: Use of legitimate administrative tools like PsExec, Cobalt Strike, Mimikatz, or vssadmin.exe to escalate privileges or delete backups.

9. Exploitation of Vulnerabilities: Exploitation of unpatched software vulnerabilities to install ransomware payloads.

10. Command-and-Control (C2) Communication: Communication with known ransomware C2 servers to receive commands or download ransomware payloads.

11. Backup Deletion or Manipulation: Ransomware often deletes or corrupts backups to make recovery harder.

12. Unexpected System Reboots or Shutdowns: Ransomware attempts to reboot or shut down systems to execute its payload or disrupt recovery efforts.

VIII. Prerequisites to Investigate Ransomware attack incident in Microsoft Sentinel

To effectively investigate a ransomware attack in Microsoft Sentinel, certain prerequisites need to be in place. These prerequisites ensure you have the necessary data, tools, and configurations to identify, analyze, and respond to such incidents efficiently.

1. Data Sources Configured: You must have the right data sources connected to Microsoft Sentinel to capture all relevant telemetry for ransomware investigation.

- **Endpoint Protection Solutions**: Integrate solutions like Microsoft Defender for Endpoint, Symantec, or CrowdStrike to capture endpoint behaviours such as process execution and file activities.
- **Identity and Access Logs:** Collect logs from Entra ID For cloud-based authentication logs and On-premises Active Directory, use Azure AD Connect or syslog integration to ingest sign-in and authentication events.
- **Network Data:** Connect firewalls, web proxies, or network monitoring tools like Palo Alto, Cisco, or Azure Network Watcher to monitor for suspicious traffic.
- **Threat Intelligence Feeds:** Enable threat intelligence feeds to identify known ransomware indicators of compromise (IOCs) such as malicious domains, IPs, or file hashes.
- **Server and Application Logs:** Ensure logs from servers and critical applications (e.g., file servers, databases) are ingested.
- **DNS and Proxy Logs:** Collect DNS query logs and outbound traffic logs to detect communication with ransomware command-and-control (C2) servers.

2. Log Analytics Workspace Configured: A properly configured Log Analytics Workspace is required for advanced hunting and querying.

- **Retention Policies:** Ensure sufficient retention (e.g., 30, 90, or 180 days) for detailed forensic investigations.
- **Custom Logs:** Ingest custom logs for unsupported devices or applications if needed.

3. Sentinel Analytics Rules: Predefined and custom analytics rules help detect ransomware activities.

- **Prebuilt Analytics Rules:** Activate rules like Mass file encryption detected, Suspicious process execution, Backup deletion attempts detected.
- **Custom Rules**: Configure custom KQL-based rules to detect organization-specific ransomware indicators.

4. Hunting Queries: Hunting queries allow for deep-dive investigations into suspicious activities.

- **Prebuilt Hunting Queries:** Use hunting queries for behaviours like Mass file modifications, Use of tools like vssadmin.exe for shadow copy deletion.
- **Custom Queries:** Build queries tailored to specific ransomware IOCs or behaviours.

5. Incident Management Configuration: Microsoft Sentinel's incident management system should be configured to support investigation and response workflows.

- **Incident Automation:** Set up playbooks to respond to ransomware alerts automatically (e.g., isolating systems, disabling user accounts).
- **Incident Triage Process:** Define escalation paths and assign responsibilities for handling ransomware incidents.

6. Role-Based Access Control (RBAC): Ensure investigators and responders have appropriate access to Microsoft Sentinel resources.

- **Required Roles:** Assign roles like **Sentinel Reader**, **Sentinel Contributor**, or **Sentinel Responder** to team members involved in investigations.
- **Access to Data Sources:** Ensure investigators can access linked data sources (e.g., Azure AD, endpoint logs).

7. Threat Intelligence Integration: Ransomware detection benefits from threat intelligence to identify IOCs quickly.

- **Enable Threat Intelligence Feeds:** Integrate threat intelligence feeds into Sentinel to match logs against known ransomware IPs, domains, and file hashes.
- **Custom Intelligence:** Import organization-specific or third-party threat feeds.

8. Response Playbooks Configured: Automated playbooks in Sentinel can assist in responding to ransomware incidents.

- **Example Playbooks:** Isolate compromised machines, Disable compromised accounts, Notify stakeholders via email or Teams.

9. Awareness of Common Ransomware Indicators: Familiarity with ransomware tactics, techniques, and procedures (TTPs) is crucial.

- **Examples of Ransomware Behaviours:** Mass file modifications, Suspicious process trees (e.g., explorer.exe → cmd.exe → ransomware.exe), Connections to C2 servers via Tor or unusual DNS queries.

IX. Investigating Ransomware Incidents in Microsoft sentinel

Investigating a ransomware attack in Microsoft Sentinel requires a systematic approach, leveraging the platform's built-in tools, analytics, and threat-hunting capabilities. Below is a step-by-step guide to investigating ransomware incidents in Microsoft Sentinel, using real-world methods and features.

1. Identify and Triage the Incident: The investigation begins with identifying the alert or incident in Microsoft Sentinel.

Locate Incident:

- Unusual file modifications (mass encryption).
- High volume of failed login attempts (possible brute force attack).
- Connections to known malicious IPs/domains.

2. Investigate the Alert Details: Click on the incident to view detailed information about the alert.

Alert Details:

Review the affected host, user account, and time of occurrence.

Identify the associated MITRE ATT&CK tactics (e.g., Initial Access, Execution, Encryption).

Evidence Details: Analyze the logs and telemetry collected, such as:

- Windows Security Logs: Event IDs related to login failures (e.g., 4625), file encryption (4663), or backup deletion.
- Azure AD Logs: Suspicious sign-ins or credential use.
- Defender for Endpoint Alerts: Behavioural indicators like "Ransomware detected."

3. Analyze Suspicious File Activities: Ransomware encrypts files in bulk, leaving indicators like file renaming, deletion, or high I/O usage**.**

- **Run File Activity Queries:** Use the Log Analytics Workspace and KQL (Kusto Query Language) to identify suspicious file operations.
- **Example Query:**
  SecurityEvent
  | where EventID == 4663
  | where ObjectName endswith ".encrypted" or ObjectName endswith ".lockbit"
  | summarize count() by Account, Computer, TimeGenerated
- **Correlate File Modifications:** Identify if files were renamed to ransomware-specific extensions like .lockbit, .crypt, .ransom.

4. Investigate User Activities: Ransomware incidents often involve compromised credentials or privilege escalation.

- **Analyze Authentication Logs:** Query Azure AD or on-premises Active Directory sign-in logs. Example Query for suspicious logins

  SigninLogs
  | where ResultType != "0"
  | summarize count() by UserPrincipalName, IPAddress, TimeGenerated

- **Review Privilege Escalation:**
  - Check if attackers escalated privileges using tools like Mimikatz or PsExec.
  - Look for Event ID 4672 (Special Privileges Assigned to New Logon).

5. Examine Suspicious Processes: Ransomware usually runs executable or script-based payloads.

- **Check Process Execution Logs:** Look for suspicious processes like powershell.exe, cmd.exe, or custom ransomware binaries.
- **Example Query:**
  SecurityEvent
  | where EventID == 4688

| where NewProcessName has_any ("ransomware.exe", "encryptor.exe", "powershell.exe")

6. Detect Backup and Shadow Copy Deletion: Ransomware often deletes backups to prevent recovery.

- **Search for Shadow Copy Deletion:** Query for the vssadmin or wmic commands in logs.
  SecurityEvent
  | where EventID == 4688
  | where NewProcessName has "vssadmin.exe"
  | where CommandLine has "delete shadows"
- **Backup Service Interruption:** Investigate if backup-related services or processes were stopped or disabled.

7. Investigate Lateral Movement: Attackers often spread ransomware across the network.

- **Check for Lateral Movement:** Use queries to detect remote command execution or SMB activity:

  SecurityEvent
  | where EventID == 4624
  | where LogonType == 3
  | where IpAddress != "<internal-IP-range>"

- **Identify Network Scanning:** Look for reconnaissance activities using tools like Nmap or SharpHound.

8. Investigate Command-and-Control (C2) Communication: Ransomware often communicates with external servers to retrieve encryption keys.

- **Analyze DNS Logs:** Check for connections to known malicious domains.

  DNSLogs
  | where QueryName endswith ".onion" or QueryName in ("malicious-domain.com")
- **Review Network Traffic:** Investigate anomalous outbound traffic, such as high-volume uploads.

9. Correlate Alerts Using Hunting Queries: Use hunting queries to correlate events and identify the full attack chain.

- **Example Hunting Query for Ransomware:**

  SecurityEvent
  | where EventID in (4625, 4688, 4663)
  | summarize count() by Account, Computer, NewProcessName, ObjectName, TimeGenerated
  | order by count() desc

- **Threat Intelligence Integration:** Match IPs, domains, or hashes with threat intelligence feeds in Sentinel.

10. Respond and Mitigate: Based on the findings, initiate an appropriate response.

- **Containment:** Isolate infected systems from the network, Disable compromised accounts.
- **Remediation:** Restore from backups, Patch vulnerabilities and strengthen defenses (e.g., apply MFA).
- **Recovery:** Decrypt files if feasible or replace encrypted data from backups.

X. Prevention and Protection Against Ransomware

1. **Regular Backups:** Regularly back up important files and data to ensure that you can recover them in case of an attack.
2. **Patch and Update:** Regularly update all software and operating systems to fix known vulnerabilities that attackers exploit.
3. **Security Awareness Training:** Educate users to recognize phishing emails and malicious attachments.
4. **Network Segmentation:** Use network segmentation to limit the spread of ransomware in case of infection.
5. **Endpoint Protection:** Implement robust endpoint security software, including antivirus and anti-malware tools.
6. **Multi-Factor Authentication (MFA):** Use MFA to protect sensitive accounts from unauthorized access.