Documenting incidents with an incident handler’s journal

Name: Hridhima Karmakar

Scenario Description:

On a Monday morning, the cybersecurity team received multiple alerts indicating unusual outbound traffic from several employee workstations. Upon investigation, it was confirmed that the company had been affected by a ransomware attack that encrypted sensitive customer and financial data. The attackers demanded payment in cryptocurrency in exchange for the decryption key.

Who caused the incident?

The incident was caused by an external threat actor who exploited a vulnerability in outdated remote desktop software. The attacker gained access through a brute-force attack and deployed ransomware across the internal network.

What happened?

Ransomware was deployed to encrypt files across the company’s shared network drives. Employees were locked out of critical systems, and a ransom note appeared on affected machines demanding Bitcoin in exchange for data recovery.

When did the incident occur?

The initial compromise likely occurred late Sunday evening when systems were less monitored. The attack was discovered on Monday morning during routine monitoring and user reports of system inaccessibility.

Where did the incident happen?

The attack primarily impacted internal systems connected to the corporate LAN, including the customer billing database, employee folders, and several department servers.

Why did the incident happen?

The incident occurred because a critical patch for the remote desktop application had not been applied, leaving the system vulnerable to brute-force attacks. Additionally, multi-factor authentication was not enforced for remote access.

Additional Notes

- What steps were taken immediately after the incident was identified?
    - Isolated infected systems from the network
    - Informed the IT response team
    - Began forensic analysis of compromised endpoints
- What could have prevented this attack?
    - Regular patch management and vulnerability scanning
    - Enforcing multi-factor authentication (MFA) for all remote access points
    - Stronger password policies and account lockout after failed attempts
- What is the next step in response and recovery?
    - Engage third-party incident response specialists
    - Evaluate backup integrity before initiating recovery
    - Begin notification process for affected stakeholders