Mitigation Recommendations Report:

When I look at the vulnerabilities I have mentioned in my previous reports and other vulnerabilities that I have not mentioned in my reports but I have done research on, first access methods such as bypassing authentication through package manipulation, remote malicious code execution, malicious code injections into various files that will run while those files are being processed to open them are used. In terms of ensuring persistence, it is especially important to set malicious applications or codes as scheduled tasks to be run when the system is started or at certain periods of daily or hourly periods through system features.Before the attack, scanning the target network system and accessing the information of the devices on that network is at the forefront. In addition, it is common to collect data such as email and personal information of employees within the organization and send malicious phishing emails. The general targets vary, but data theft and ransom attacks are at the forefront. Here are some suggestions that can be made against these attacks:

- Actively monitor system network traffic: This method allows you to detect abnormal requests to the system network or abnormal movements within the network.
- Follow the updates of systems and software within the organization: Especially making security patches that come with updates helps to close vulnerabilities in the system.
- If possible, limit operations within the network: With this method, it can be difficult for the attacker to move within the network. In this way, even if he infiltrates a system, he cannot easily access other systems, or he can be prevented from leaking information or executing remote commands.
- Informing employees within the organization about cyber security: In this way, the attacker can be prevented from achieving success with such methods, especially by being knowledgeable and competent about the storage of personal information and phishing emails.
- Carefully setting authorization limits for accounts on systems: This will limit what an attacker can do even if they take over an account in the system, they will have to find other accounts and try to take them over to achieve their goals, so they are more likely to be detected, but they can limit the damage to the system until they are detected.
- Updating firewall policies to keep up to date: With this method, a security system adapted to current situations is established. Thus, measures can be taken against current threats.
- Using firewall, IPS/IDS solutions: By using these solutions, movements on the network and systems can be monitored, attacks can be detected and prevented.
- Regular monitoring of system logs: With this method, an abnormal movement within the system can be detected.
- Following the latest security reports: Keeping up to date with current threat information makes it easier to take precautions against the latest threats.

- Closing unused ports: This prevents the risks posed by ports that may be used by an attacker but overlooked by system administrators.