Recent Significant Malware Incidents: attack methods and mitigation

1. Lazarus Group's "Operation SyncHole" against South Korean organizations
   Attack Techniques:
   Watering Hole Attack: The attackers took over legitimate South Korean online media sites visited by target organizations.
   Exploiting Vulnerabilities: They exploited publicly known vulnerabilities in software specific to South Korea, such as Innorix Agent, which is typically required for South Korean online banking and government services.
   Lateral Movement: The Lazarus Group employed tools such as the Innorix Abuser to take advantage of vulnerabilities and perform lateral movement within the victim network, downloading and running further malware such as ThreatNeedle.
   Custom Malware: They used custom malware implementations such as ThreatNeedle, wAgent, SIGNBT, and COPPERHEDGE, designed to steal information, create persistence, and perform internal reconnaissance.
   Legitimate Software Abuse: The threat actors misused legitimate tools such as SyncHost.exe and Innorix Agent to inject and load malware, complicating detection.
   Mitigation and Resolution:
   Threat Intelligence Sharing: Security researchers provided insights with the Korea Internet & Security Agency (KrCERT/CC) facilitating rapid response.
   Patching and Updating: Vendors issued patches to rectify the exploited vulnerabilities within the South Korean software.
   Endpoint Protection: EDR and antivirus tools are utilized by organizations to detect and prevent the execution of malware.
   Security Audits: Regular security audits and vulnerability assessments of important systems and networks, especially database servers, are advised to be conducted ahead of time to identify and resolve vulnerabilities.

2. RansomHub ransomware against education and other vital industries
   Attack Methods:
   Initial Entry: Initial access by RansomHub affiliates usually comes through the exploitation of internet-facing systems' vulnerabilities, phishing emails, or password spraying attacks.
   Exploitation of Vulnerabilities: They use publicly disclosed vulnerabilities like Zerologon (CVE-2020-1472) and Citrix ADC (CVE-2023-3519) to establish a foothold in the network.
   Lateral Movement and Privilege Escalation: They utilize tools such as Mimikatz, PsExec, and remote access tools (e.g., AnyDesk, Splashtop) after gaining entry to move laterally across the network and privilege escalate.

Defense Evasion: RansomHub utilizes evasion techniques such as disabling security tools through tools such as EDRKillShifter, TDSSKiller, and altering registry configurations.
Data Exfiltration and Encryption: Affiliates exfiltrate sensitive information prior to encrypting data using robust encryption methods such as Curve25519 and AES, using double extortion techniques.
Shadow Copy Deletion: They remove volume shadow copies to prevent recovery attempts.
Mitigation and Resolution:
Patch Management: Apply security updates and patches for operating systems, software, and firmware on a regular basis, focusing on known exploited vulnerabilities.
Multi-Factor Authentication (MFA): Use MFA on all remote and privileged access points to block credential-based attacks.
Network Segmentation: Use network segmentation between IT and operational technology (OT) networks and key systems to restrict lateral movement.
Secure Backups: Keep offline, immutable, and encrypted backups of important data, and periodically test restoration processes.
Endpoint Protection: Deploy and set up EDR tools to identify and stop ransomware behavior.
User Awareness Training: Implement security awareness training to ensure employees can identify phishing attacks and unusual behavior.

3. Akira ransomware attacking Windows, Linux, and ESXi environments
Attack Methods
Initial Access: Akira achieves initial access mainly by taking advantage of weaknesses in VPNs that do not have multi-factor authentication (MFA), spear-phishing operations, stolen credentials, and taking advantage of weaknesses in public-facing applications.
Credential Harvesting: They employ tools such as Mimikatz and LaZagne to get authentication credentials, which consist of NTLM hashes and plaintext passwords.
Lateral Movement: Akira uses lateral movement throughout the network, employing legitimate tools such as AnyDesk and PowerShell scripts to disable antivirus software and remove volume shadow copies.
Double Extortion: They utilize a double extortion scheme by exfiltrating sensitive information prior to encrypting it and threatening to release the stolen information on their Tor-hosted leak site unless the ransom is paid.
Encryption: The ransomware utilizes powerful encryption algorithms, including ChaCha20 and RSA, to encrypt files, usually appending a '.akira' extension.
Mitigation and Resolution:
Isolate Infected Systems: Suspend affected devices from the network at once to avoid the ransomware from propagating further and to maintain forensic evidence.
Incident Response Activation: Activate internal or external incident response groups to evaluate the effect of the attack, identify the entry point, contain the threat, and eliminate the malware.
Secure Data Backups: Store offline and immutable backups of vital information to facilitate successful recovery without the need for paying the ransom.

Patch and Update Systems: Periodically install security patches and updates for operating systems, software applications, and network devices, particularly for VPNs and other well-known vulnerabilities.
Enforce Strong Authentication: Deploy and require multi-factor authentication (MFA) for all user accounts, VPNs, and application services to stop credential-based attacks.
Endpoint Protection and EDR: Install and set up EDR solutions with particular ransomware detection rules to track and prevent ransomware activity in real time.
Security Awareness Training: Educate employees to identify and report suspicious emails, links, and unusual behavior that may be signs of a ransomware attack.
Network Segmentation: Use network segmentation to restrict lateral movement within the network.