1. Lovable AI Website Builder Exploited for Phishing Campaigns

Attack Method:
 Since February 2025, cybercriminals have exploited Lovable, an AI-powered website builder, to create phishing sites, malware loaders, and fraudulent websites. These sites were distributed via phishing emails targeting multi-factor authentication (MFA) systems and cryptocurrency wallets. One major campaign in February affected over 5,000 organizations .

Resolution:
 Lovable responded swiftly by taking down a major phishing cluster within a week of discovery. They implemented AI-driven real-time detection systems to block malicious website creation and initiated automated daily scans to identify and flag suspicious content .

2. Akira Ransomware Targets Global Organizations

Attack Method:
 The Akira ransomware group has been active since March 2023, targeting over 250 entities, including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. They deploy ransomware-as-a-service, encrypting data and demanding ransoms for decryption keys .

Resolution:
 Organizations affected by Akira ransomware have been advised to follow best practices for ransomware response, including isolating infected systems, restoring from backups, and reporting incidents to relevant authorities. Specific details on decryption tools or recovery methods are not publicly disclosed.

3. Kettering Health Disrupted by Nefarious Mantis Ransomware

Attack Method:
 In May 2025, Kettering Health, a healthcare provider in Ohio, suffered a system-wide outage due to a ransomware attack attributed to the Nefarious Mantis group. The attack disrupted patient care systems, leading to the cancellation of elective procedures and forcing the organization to suspend phone-based payment requests .

Resolution:
 Kettering Health worked with cybersecurity experts and law enforcement to contain the attack and restore systems. They implemented enhanced security measures to prevent future incidents and communicated with patients about the status of services and potential scams.