Athira Biju
Amal Jyothi College of Engineering

1. GhostTouch Exploit, Non-contact Screen Hijacking

Type: Electromagnetic Injection | Sector: Consumer Devices

• Attack Method:

o Attackers used electromagnetic interference to simulate touch events on capacitive screens without physical contact.

o Targets included unattended smartphones, ATMs, and public kiosks.

o The exploit could unlock devices, approve transactions, or install apps silently.

• Mitigation:

o OEMs began testing EM shielding and recalibrating firmware.

o Security researchers advised disabling touch input when idle or using screen covers.

o No mass exploitation was reported, but the proof-of-concept led to hardware-level defenses.

2. ShadowLoader in CI/CD Pipelines, Supply Chain Backdoor

Type: Fileless Malware | Sector: DevOps & Cloud Infrastructure

• Attack Method:

o Discovered in early 2025, ShadowLoader embedded itself in CI/CD pipelines, such as Jenkins and GitHub Actions.

o It used obfuscated YAML scripts and hijacked environment variables to inject payloads during build processes.

o The malware never touched the disk, making it invisible to traditional antivirus tools.

• Mitigation:

o DevOps teams implemented stricter script validation and created sandboxed build environments.

o GitHub and GitLab rolled out better pipeline scanning tools.

o This incident led to new best practices for secure automation workflows.

3. SilkSpider, Steganographic Malware in Textile Design Files

Type: Steganography-based Malware | Sector: Fashion & Manufacturing CAD Systems

TASK 5

Athira Biju
Amal Jyothi College of Engineering

- **Attack Method:**
  - o Malware was hidden inside .DST and .EMB embroidery design files used in textile CAD software.
  - o When opened in vulnerable software, the embedded code triggered remote access trojans, or RATs.
  - o It targeted high-end fashion houses and textile exporters in Southeast Asia.
- **Mitigation:**
  - o Vendors fixed parsing engines and added file integrity checks.
  - o Affected companies isolated design workstations and used behavioral monitoring.
  - o There was increased awareness about niche file formats as attack vectors.