TASK 5
Submitted By :
Sreehari Vinod

1. “InkDrop” - Malware Hidden in Printer Firmware Updates

Type: Firmware-Level Malware | Sector: Office Hardware & IoT

Attack Method:

Attackers compromised third-party printer driver repositories and injected malware into firmware update packages. When installed, the malware created persistent backdoors through USB-connected printers, allowing movement within corporate networks. It bypassed endpoint protection by operating at the firmware level, below OS visibility.

Mitigation:

Affected vendors issued signed firmware updates and revoked compromised certificates. Organizations were advised to isolate printer networks and disable auto-updates. This triggered a shift toward checking hardware integrity in enterprise environments.

2. “CacheCrush” - Browser-Based Side-Channel Attack via Shared CPU Caches

Type: Side-Channel Exploit | Sector: Web Browsers & Cloud Platforms

Attack Method:

CacheCrush exploited shared CPU cache behavior in multi-tenant cloud environments. Malicious JavaScript running in a browser could infer sensitive data from other browser tabs or virtual machines by measuring cache access times. It bypassed sandboxing and didn't require direct access to the victim’s session.

Mitigation:

Browser vendors, including Chrome and Firefox, implemented stricter timing APIs and cache partitioning. Cloud providers initiated microarchitecture-aware VM scheduling. There was increased awareness about hardware risks in virtualized environments.

3. “MetaMorph” - Polymorphic Malware in AI Model Weights

Type: AI-Embedded Malware | Sector: Machine Learning & Research Labs

Attack Method:

MetaMorph embedded malicious payloads inside the weight matrices of pre-trained AI models, like PyTorch and TensorFlow. When loaded into memory, the model executed hidden shellcode through custom activation functions. It spread through academic repositories and open-source model hubs.

Mitigation:

Machine learning platforms added checksum validation and sandboxed model execution. Researchers began scanning model weights for unusual patterns. This led to new guidelines for sharing and reproducing secure machine learning models.