1. TamperedChef Credential-Stealing Malware via Fake AppSuite PDF Editor

Attack Method

- Malicious actors created fake websites spoofing "AppSuite PDF Editor" and launched them using Google Ads campaigns starting late June 2025.
- Users were tricked into downloading a trojanized version of the PDF editor. The malware, “TamperedChef,” remained dormant for ~56 days—matching the length of Google Ad campaigns—before activation.
- Once active, it established persistence via Windows Registry tweaks and scheduled tasks. It harvested browser credentials and session cookies by terminating browser processes and exploiting Windows DPAPI. It also performed reconnaissance to bypass security defenses and acted as a backdoor for future payloads.

Mitigation/Resolution

- Security researchers (Truesec) identified the campaign and warned users, enabling them to avoid the malicious downloads.
- Best practices to mitigate such threats include: downloading software only from official sources, verifying URLs carefully, using ad blockers or safe browsing tools, and maintaining up-to-date antivirus/antimalware protection.

2. Gayfemboy—Mirai-based Botnet Targeting IoT Devices

Attack Method

- “Gayfemboy” is a Mirai-derived botnet first discovered in February 2024, which emerged more prominently in 2025.
- It infiltrates devices like routers (Cisco, TP-Link, ASUS, Vivo, Zyxel, Realtek) by exploiting vulnerabilities—including unauthenticated Redis servers—and initiates cron jobs executing shell scripts.

- The malware disables SELinux, blocks external access to Redis ports to prevent competitors, terminates competing mining processes, renames files, evades sandboxes, binds to UDP port 47272, executes DDoS attacks (UDP, TCP, ICMP), and enables backdoor control.

- It uses playful strings (“twinks :3,” “meowmeow”) and C2 domains like “i-kiss-boys.com”—a tactic to evade detection.

Mitigation/Resolution

- Fortinet deployed multi-layered protection via FortiGuard—blocking identified C2 (command-and-control) domains with web filtering and deploying IPS signatures against exploited vulnerabilities.

- Recommendations include patching vulnerable IoT and networking devices, disabling unused services like open Redis ports, using strong authentication, segmenting networks, and using network-based filtering to detect malicious activity.

---

3. WhatsApp “Zero‑Click” Exploit Targeting iPhones (CVE‑2025‑55177 + CVE‑2025‑43300)

Attack Method

- A highly sophisticated, **zero-click exploit** was discovered in WhatsApp (CVE‑2025‑55177), combined with an Apple OS vulnerability (CVE‑2025‑43300). It allows attackers to deliver spyware simply by sending a message—no user interaction required.

- The exploit targeted specific individuals (including civil society members) over a three-month period.

Mitigation/Resolution

- WhatsApp issued advisories, urging users to update to minimum safe versions: **WhatsApp v2.25.21.73** for iOS and **v2.25.21.78** for macOS.

- Affected users were advised to perform a **full factory reset**.

- Additional protections: enable **iOS Lockdown Mode** or **Android’s Advanced Protection Mode** to guard against such advanced threats.