مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Android Spyware LANDFALL Exploiting Samsung Devices

Tracking #:432317979

Date:10-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a sophisticated Android spyware campaign named LANDFALL has been uncovered, targeting Samsung Galaxy devices by exploiting zero-day vulnerabilities in Samsung's Android image processing library.

TECHNICAL DETAILS:

A sophisticated Android spyware campaign named LANDFALL has been uncovered, targeting Samsung Galaxy devices by exploiting zero-day vulnerabilities in Samsung's Android image processing library. Notably, the primary vulnerability (CVE-2025-21042) was exploited via malicious DNG image files delivered through messaging platforms such as WhatsApp. The campaign exhibited advanced surveillance capabilities, remained undetected for months, and aligns with patterns observed in commercial spyware operations active in the Middle East. Samsung patched the critical vulnerabilities in April and September 2025, but historic exploitation highlights the ongoing threat posed by rapidly evolving mobile spyware and the importance of immediate updates and robust endpoint security.

Details
Vulnerabilities

- CVE-2025-21042:
  - Critical zero-day in Samsung's image-processing library (libimagecodec.quram.so)
  - Enabled arbitrary code execution by parsing malformed DNG (Digital Negative) image files with an embedded ZIP archive.
  - Exploited in the wild from July 2024 until patch release in April 2025.
- CVE-2025-21043:
  - Related zero-day in the same Samsung image library, patched in September 2025.
  - Shares attack patterns with CVE-2025-21042, delivered via DNG images through messengers.
- Related iOS/WhatsApp CVEs:
  - Apple CVE-2025-43300 (DNG parsing) and WhatsApp CVE-2025-55177 exploited similarly in iOS environments in parallel campaigns in 2025.

Attack Chain & Techniques

- Initial Delivery:
  - Malicious DNG image files crafted to exploit Samsung's image library.
  - Distributed through WhatsApp, leveraging naming patterns like "WhatsApp Image ...jpg".
- Exploit Chain:
  - Zero-click vector: Victim need not interact directly with the media.
  - DNG files embedded with ZIP archives extract two spyware modules:
    - Loader (b.so): ARM64 ELF shared object, acts as the primary surveillance backdoor.
    - SELinux Manipulator (l.so): Elevates privileges and establishes persistence by manipulating device security policies.
- Capabilities:
  - Comprehensive device surveillance: audio recording, call/SMS collection, contact and photo extraction, location tracking, app inventory, network analysis, and more.

- Detection evasion: anti-debugging checks, Frida/Xposed detection, custom C2 protocol, and certificate pinning for command and control (C2).
- Targets & Attribution:
  - Targeted Samsung device models: Galaxy S22/S23/S24, Z Fold4, Z Flip4 series.
  - Observed targeting in Middle east Countries
  - Infrastructure shares traits with known PSOA spyware (notably Stealth Falcon and Variston), though no direct attribution has been established.

Indicators of Compromise:

Malware Samples: A list of malware samples for LANDFALL activity is listed below

SHA256 Hash	Filename
b06dec10e8ad0005ebb9da24204c96cb2e297bd8d418bc1c8983d066c0997756	img-20250120-wa0005.jpg
c0f30c2a2d6f95b57128e78dc0b7180e69315057e62809de1926b75f86516b2e	2.tiff
9297888746158e38d320b05b27b0032b2cc29231be8990d87bc46f1e06456f93	whatsapp image 2025-02-10 at 4.54.17 pm.jpeg
d2fafc7100f33a11089e98b660a85bd479eab761b137cca83b1f6d19629dd3b0	b.so
384f073d3d51e0f2e1586b6050af62de886ff448735d963dfc026580096d81bd	
b975b499baa3119ac5c2b3379306d4e50b9610e9bba3e56de7dfd3927a96032d	1.jpeg
a62a2400bf93ed84ebadf22b441924f904d3fcda7d1507ba309a4b1801d44495	
29882a3c426273a7302e852aa77662e168b6d44dcebfca53757e29a9cdf02483	img-20240723-wa0001.jpg
2425f15eb542fca82892fd107ac19d63d4d112ddbfe698650f0c25acf6f8d78a	6357fc.zip
b45817ffb0355badcc89f2d7d48eecf00ebdf2b966ac986514f9d971f6c57d18	img-20240723-wa0000.jpg
69cf56ac6f3888efa7a1306977f431fd1edb369a5fd4591ce37b72b7e01955ee	localfile~
211311468f3673f005031d5f77d4d716e80cbf3c1f0bb1f148f2200920513261	l
ffeeb0356abb56c5084756a5ab0a39002832403bca5290bb6d794d14b642ffe2	

IP Addresses

- 45.155.250[.]158
- 46.246.28[.]75
- 91.132.92[.]35
- 92.243.65[.]240
- 192.36.57[.]56
- 194.76.224[.]127

Domain Names

- brightvideodesigns[.]com
- healthyeatingontherun[.]com

- hotelsitereview[.]com
- projectmanagerskills[.]com

RECOMMENDATIONS:

1. Immediate Actions:
   - Ensure all Samsung Galaxy devices have the latest security updates (April 2025 and later).
   - Patch management: Apply firmware and security updates as soon as they are released by Samsung and relevant vendors.
2. Detection and Response:
   - Deploy advanced endpoint security products that detect zero-day exploits and spyware (e.g., Advanced WildFire, Advanced Threat Prevention).
   - Block known LANDFALL C2 domains and monitor for associated DNG file hashes.
   - Hunt for indicators of LANDFALL infection using listed IoCs and monitor for anomalous HTTPS traffic to suspicious ports/domains.
3. Prevention:
   - Educate users not to open images or attachments from untrusted or unknown sources, even via familiar apps like WhatsApp.
   - Leverage network-layer security (Advanced DNS Security, URL Filtering) to detect and prevent contact with malicious infrastructure.
   - Limit exposure by enforcing least-privilege access on mobile devices and utilizing mobile device management (MDM) solutions.
4. For Security Teams and SOCs
   - Review logs and telemetry for evidence of policy manipulation or exploitation of vulnerable Samsung devices.
   - Integrate LANDFALL's known IoCs and C2s into SIEMs and threat intelligence platforms.
   - Monitor for new exploit disclosures involving image parsing (TIFF/DNG) across all mobile platforms.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://unit42.paloaltonetworks.com/landfall-is-new-commercial-grade-android-spyware/