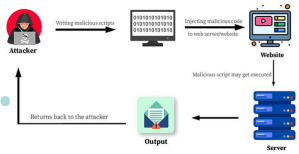
INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC
DOI No. 10.5281/zenodo.15689499
MAY 2025

CYBER BULLETIN

Digital Espionage & Surveillance

1. Pegasus 2.0 Spyware



REMOTE CODE EXECUTION

TARGET: Politicians, journalists and dissidents in Europe and North Africa.

IMPACT: Zero-click iOS exploit allows full device control calls, messages, microphone and camera compromised. Used in covert political surveillance operations.

MITIGATION: Use Lockdown Mode on iPhones, update iOS to latest version & monitor network traffic for anomalies.

2. GravityRAT Malware

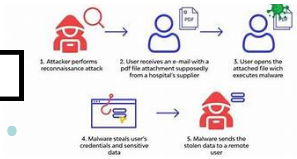
TROJANIZED ANDROID

TARGET: Android users in South Asia.

IMPACT: Disguised as encrypted messengers, the spyware steals call logs, GPS data and files. Links to Pakistan-based threat actors and suspected state involvement.

MITIGATION: Avoid sideloading APKs, install only from trusted sources & review app permissions.

3. Chinese APTs Exploit LinkedIn



SOCIAL ENGINEERING

TARGET: Defense contractors, security analysts & government employees.

IMPACT: Fake LinkedIn profiles used to establish trust and extract sensitive info through casual conversations and document sharing.

MITIGATION: Verify unknown connections, educate employees on social media threats and monitor data leaks.

4. FinSpy Backdoors

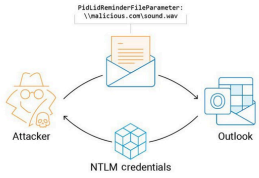
iMESSAGE EXPLOIT VECTOR

TARGET: iOS users involved in legal, political and media sectors.

IMPACT: Vulnerability (patched in March 2025) allowed remote takeover through a single iMessag, part of a larger spyware suite.

MITIGATION: Update to latest iOS, enable Lockdown Mode and disable message previews.

5. Zero-Click iMessage Spyware



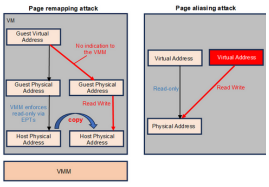
ZERO-CLICK EXPLOIT

TARGET: Human rights activists & NGO workers in MENA region.

IMPACT: Keylogging, remote surveillance and webcam access. It remains hidden using rootkit-level stealth.

MITIGATION: Use secure operating systems (like Tails), enable BIOS/UEFI security and detect abnormal behavior via logs.

6. NSO Spyware Resurfaces



ALIAS-BASED LICENSING

TARGET: Foreign journalists and opposition leaders.

IMPACT: Leaked documents reveal new spyware being licensed under aliases to avoid restrictions. Reignites debate on surveillance ethics.

MITIGATION: Use encrypted, ephemeral messaging apps, rotate devices regularly & avoid Wi-Fi in sensitive areas.

INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC
DOI No. 10.5281/zenodo.15689499
MAY 2025

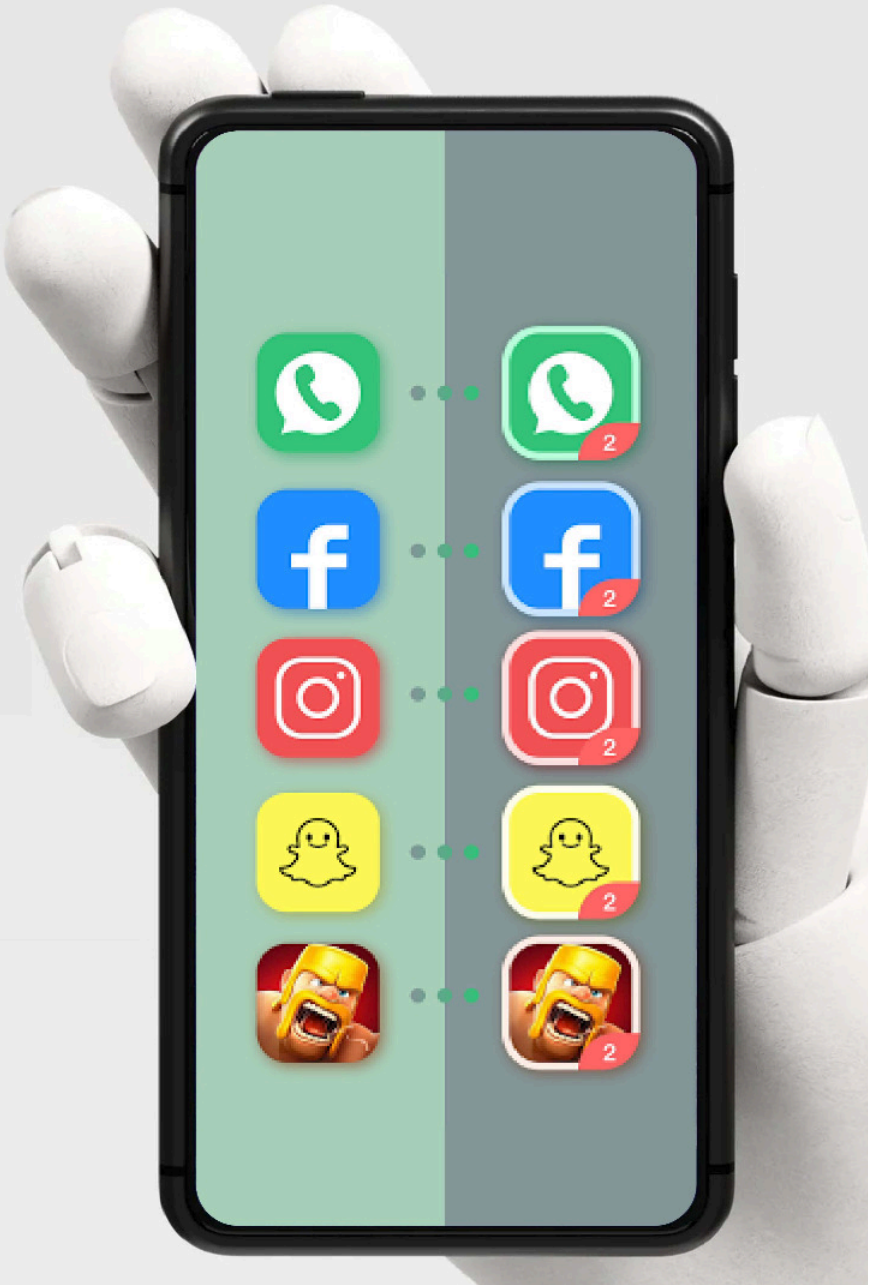
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा पक्का

CYBER SECURITY
POSTER OF THE DAY

Avoid downloading cloned versions of popular apps they often contain malware



#AppClones
#MalwareAlert

CYBER SAKCHHARTA ABHIYAN
UNDER THE AEGIS OF
CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION

FACULTY COORDINATORS
MR. SHUBHAM KUMAR | MR. FAIZAN MAHMOOD | MR. MOHD TALHA
STUDENTS COORDINATORS
MOHAMMAD FARHAN | SIDRA SIDDIQUI | ELMA SHARIQ
AREEBA KHAN | ANAMTA ANSARI

Prof.(Dr.) MOHAMMAD FAISAL
Head, Department of Computer Application