Subject:- **Threat Actors Spying on iPhones Through Zero-Click Spyware (Advisory No. 42)**

Context. Reportedly, threat actors are targeting iPhones with zero-click spyware; multiphase polymorphic and self-destructive malware. The campaign is considered as part of sophisticated and long-running mobile espionage and data exfiltration activity termed as ***Operation Triangulation***.

2. **International View Point**. Operation Triangulation has recently been unearthed, however, it was running since 2019. Russia has accused USA and Apple for facilitating spying activities, though Apple has denied such allegations. It may be inferred that the operation is to spy Russian officials iPhones.

3. **Modus Operandi**. Technical details and modus operandi of Operation Triangulation are as follows:

a. During initial phase, victims are infected using zero-click exploits via the iMessage platform. Malware runs with root privilege, gaining complete control of the victim's devices and data.

b. Attack begins with iOS devices receiving a message via iMessage containing malicious attachment.

c. As it is a zero-day, the message triggers malware execution automatically without any user interaction and notice.

d. The malware downloads payloads from download server and further exfiltrates victim’s data to under mentioned remote servers:

(1) backuprabbit.com
(2) businessvideonews.com
(3) cloudsponcer.com
(4) mobilegamerstats.com
(5) snoweeanalytics.com
(6) tagclick-cdn.com
(7) topographyupdates.com
(8) unlimitedteacup.com
(9) virtuallaughing.com
(10) web-trackers.com
(11) growthtransport.com
(12) Addatamarket.net

(13) datamarketplace.net
(14) anstv.net
(15) ans7tv.net

e. In the final phase, both the initial iMessage text and malicious attachment are deleted automatically to erase traces (crafted evasion). Most recent version, which has been successfully targeted is iOS 15.7.

4. **Recommendations**

a. All iPhone users are advised to update to latest versions (iOS 16.4.1 or above).

b. Keep iMessages off/blocked.

c. Avoid storing official data/correspondence in mobile phone.

d. Remote C&C servers domains/URLs at Para 3d (serial 1 to 15) be blocked at firewall by administrators.