GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

12 Januari 2026

Advaes namba 112: *Commercial Spyware* we i Stap Tagetem Ol Yusa blong ol Mobael Mesej Aplikesen

Deit we hemi rilis: 25 Novemba 2025
Impak: HAE / KRITIKOL
TLP: KLIA

Dipatmen blong Komunikesen mo Dijitol Transfomesen (DKDT) tru long CERT Vanuatu (CERTVU), i givimaot advaeseri ia.

Woning ia hem i blong olgeta Oganaesesen mo Sistem/Netwok Administreta we oli yusum prodak ia. Woning ia oli mekem blong olgeta teknikol yusa mo sistem administreta oli andastanem.

Wanem ia?

Commercial spyware (we oli kolem tu se "*commercial-grade*" o "*surveillance*" *spyware*), hem i rifea long ol *off-the-shelf* o *brokered* tul blong seveilens we oli salem long gavman o ol praevet institusen we oli pem we oli save monitarem mo kontrolem ol mobael divaes long wan rimot fasin. Ol denjares akta ia oli stap yusum ol tul ia blong tagetem ol yusa blong mesej aplikesen tru long fasin blong hakem ol akaon mo delivarem rabis sofwea o ol monitaring implant we i stilim o spae long ol mesej, ol kol, ples, media, mo ol narafala sensitiv data.

Hemia i afektem wanem Sistem?

Hem i no stop nomo long wan aplikesen o OS: Ol kampen ia oli tagetem ol yusa blong plante mesej aplikesen (*Signal, WhatsApp, Telegram*, mo samfala moa) long ol mobael platfom (*Android* mo *iOS*) mo oli save eksploitem ol vulnerabiliti blong ol platfom o aplikesen ia antap long sosol enjiniaring.

Hemia i minim wanem?

Olsem wanem ol ataka oli eksploitem vulnerabiliti ia (atak vekta)

1. ***Phishing & malicious QR / device-linking codes*:** Ol ataka oli sendem ol link o QR kod we, taem oli skanem o klik long olgeta, hemi linkim akaon blong viktim long wan divaes we ataka i kontrolem o hem i mekem ol yusa oli instolem ol rabis app/*dropper installers*.
2. ***Zero-click exploits*:** Ol eksploit we i no nidim eni interaksen blong yusa (olsem eksampol, wan mesej o media we oli krietem) oli save delivarem ol spaewea long wan kwaet fasin mo oli gud tumas long saed blong kompromaesem ol spesifik taget.
3. ***Impersonation / trojanized apps*:** Ol ataka oli krietem ol rabis aplikesen o web pej mo oli giaman sendem ol mesej long ol mesej platfom blong trikim ol viktim blong instolem ol spaewea. Taem oli instolem finis, spaewea ia i abyusum ol pemisen o platfom aspek blong stilim o muvum ol data mo spredem long ol kontak.
4. ***Follow-on-exploitation*:** Afta long fes akses long wan akaon o divaes, ol ataka bae oli mekem moa *payloads* (olgeta we oli stap kolektem ol kredensol, ol *persistent implants*, ol data eksfiltresen modiul) blong mekem akses mo tingting blong olgeta i moa strong.

Proses blong Katem Daon Risk

CERTVU i rikomendem se:

- Apdeitem OS mo ol App kwiktaem.
- Instolem ol App nomo long ol stoa we oli trastem.
- Onem malti-fakta / sistem blong tu-step verifikesen.
- No mas skanem ol QR kod / link we oli no trastem

Refrens

1. https://thehackernews.com/2025/08/whatsapp-issues-emergency-update-for.html
2. https://unit42.paloaltonetworks.com/landfall-is-new-commercial-grade-android-spyware/
3. https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger/