# Intelligence russa e app di messaggistica: il phishing ora punta alle chiavi di backup di Signal



L’intelligence ucraina conferma e amplia l’allarme statunitense: i servizi russi non rompono la crittografia delle app di messaggistica, ma convincono le vittime a consegnare le chiavi che proteggono i loro backup. Il bersaglio sono funzionari, militari, politici e attivisti in Ucraina, Europa e Stati Uniti. La svolta operativa più recente riguarda in modo specifico Signal; WhatsApp rientra nel quadro più ampio di *targeting*, non in questa singola tattica.

Il 27 giugno il Servizio di Sicurezza dell’Ucraina (SSU) ha reso noto, in un comunicato su Telegram, di avere ricostruito insieme all’FBI una campagna di lungo corso condotta dai servizi di intelligence russi per violare gli account di messaggistica di obiettivi ad alto valore informativo. Lo SSU non attribuisce l’attività a uno specifico gruppo, ma la inquadra come operazione sistematica di spionaggio: l’obiettivo dichiarato è accedere a informazioni militari, politiche ed economiche scambiate dagli utenti e sottrarne i dati personali. La tecnica di ingresso è un SMS che si finge il *bot* di assistenza della piattaforma e induce la vittima a rivelare le proprie credenziali.

La comunicazione ucraina arriva il giorno dopo l’aggiornamento congiunto FBI e CISA del 26 giugno, l’avviso
I-062626-PSA
, che rivede il precedente PSA di marzo e introduce l’elemento operativo più rilevante. Gli attori non si limitano più a carpire codici di verifica o PIN dell’account, né a collegare

dispositivi controllati dall’aggressore: ora puntano a farsi consegnare la *Backup Recovery Key*, la chiave che cifra la copia di backup delle conversazioni. Chi ottiene quella chiave può ripristinare il backup, leggere la cronologia di messaggi privati e di gruppo e prendere il controllo dell’account.

## Il punto tecnico: non è una falla di Signal

L’FBI è esplicito su un aspetto che conviene tenere fermo per non amplificare letture distorte: gli attori hanno compromesso singoli account, non la crittografia delle applicazioni né le applicazioni stesse. Il perimetro violato è quello del recupero e del backup, non quello del protocollo *end-to-end*. La leva resta l’inganno: i messaggi-esca riprodotti nell’avviso si presentano come comunicazioni ufficiali di Signal e guidano passo passo l’utente a generare la chiave di recupero e a incollarla in chat, con la promessa di evitare la perdita di messaggi o di sincronizzare un backup a rischio.

Il flusso documentato dall’FBI presuppone due passaggi: prima la vittima attiva il backup seguendo la finta comunicazione (Figura 1 dell’avviso, etichettata *Sample Phishing Message 1*), poi consegna la chiave di recupero (Figura 2). Entrambi i messaggi-esca ricalcano i passaggi dell’interfaccia di Signal (impostazioni, backup, visualizzazione della chiave), e proprio per questo la nuova tattica delle chiavi di backup va circoscritta a Signal, mentre il riferimento a WhatsApp resta valido per la campagna nel suo insieme.

C’è un dettaglio che alza la posta sul piano della persistenza. Se la vittima condivide la *Backup Recovery Key*, quella chiave resta valida anche dopo la ricreazione dell’account sullo stesso numero di telefono: l’aggressore potrebbe quindi rientrare in un secondo momento. L’unica contromisura indicata è generare una nuova chiave nelle impostazioni, operazione che invalida la precedente per i

download futuri; resta però il fatto che un backup già scaricato dall'attaccante non si annulla. La separazione tra ciò che si può ancora proteggere e ciò che è già compromesso è netta, e va comunicata con altrettanta chiarezza agli utenti a rischio.

## Attribuzione e nomi cluster

Sul fronte dell'attribuzione conviene muoversi con cautela, perché le diverse fonti usano etichette diverse. L'FBI parla di più *cluster* riconducibili ai servizi russi (RIS), tra cui ufficiali dell'FSB inseriti nella Guardia di Frontiera e soggetti che operano per conto delle forze militari, e li traccia pubblicamente come UNC5792
e UNC4221
. Lo SSU, dal canto suo, non nomina un gruppo. Le ondate di attacco analoghe contro utenti Signal e WhatsApp sono state ricondotte in letteratura ai cluster noti come *Star Blizzard*, UNC5792
(parzialmente sovrapponibile a UAC-0195
per il CERT-UA) e UNC4221
(equivalente a UAC-0185
): nomenclature da incrociare con prudenza, perché la stessa attività può comparire sotto sigle differenti a seconda del fornitore di *intelligence* o dell'agenzia nazionale.

Va segnalato anche un punto su cui è facile inciampare leggendo l'avviso: la frase che attribuisce gli attacchi a *hacker* dall'Iran e da Paesi post-sovietici non è una valutazione dell'FBI, ma testo del messaggio-esca riprodotto nell'avviso, ossia parte stessa della truffa.

## Perché interessa lettori europei e italiani

La campagna non è un fatto di cronaca confinato al fronte

ucraino. L’FBI include tra i bersagli funzionari governativi statunitensi e internazionali, personale militare, figure politiche e giornalisti; lo SSU estende esplicitamente il perimetro a Europa e Stati Uniti, e anche a profili personali di cittadini ucraini.

Per chiunque, in ambito istituzionale, di difesa o giornalistico europeo, usi le app di messaggistica come canale di lavoro, il modello di rischio cambia: la superficie da presidiare non è la cifratura del messaggio, ma il ciclo di vita di sessioni attive, backup e chiavi di recupero. È lo stesso terreno su cui si gioca, da anni, la sicurezza della messaggistica sicura, e che il cyber spionaggio russo ha imparato a sfruttare combinando ingegneria sociale e infrastruttura di intelligence.

Le indicazioni difensive restano elementari ma dirimenti: rivedere periodicamente le sessioni attive e disconnettere i collegamenti sconosciuti, attivare la verifica a due fattori, non scansionare QR ricevuti da utenti non noti e, soprattutto, non comunicare mai codici di conferma, PIN, password o chiavi di recupero, per quanto la richiesta appaia urgente o ufficiale. Come ricorda l’FBI, l’assistenza legittima delle app non chiede codici dentro l’applicazione e non invia link per verificare o ripristinare un account.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/intelligence-russa-chiavi-di-backup-messaggistica/