Video virali su TikTok come vettori di malware



Negli ultimi anni i **video virali** su TikTok – specie quelli promossi come “trucchi” per sbloccare funzioni premium o filtri magici – sono stati sfruttati da cybercriminali per diffondere **malware** (inclusi **trojan** e info-stealer). Alcuni casi reali documentati hanno mostrato come utenti attratti da promesse di *software gratis* siano stati istruiti, direttamente nei video, a eseguire comandi PowerShell dannosi o a scaricare app contraffatte.

Video Virali TikTok usati per diffondere malware e trojan

Per esempio, Trend Micro ha individuato una campagna in cui video (spesso creati con voce e presentazione generata da IA) invitavano gli utenti a premere “Windows+R”, avviare PowerShell e inserire un comando che in realtà scaricava e lanciava trojan **Vidar** e **StealC**. In un caso il video – che prometteva di “boostare” Spotify o attivare Windows gratis – ha raggiunto oltre mezzo milione di visualizzazioni. Similmente, **Trend Micro** e BleepingComputer hanno descritto come questi video sfruttino l’“algoritmo virale” di TikTok per massimizzare la portata: ogni clip è pubblicata su account fasulli e presto sparisce, ma intanto inducono decine di migliaia di utenti a seguire istruzioni che portano all’installazione di malware.

Un altro caso documentato riguarda la cosiddetta **Invisible Challenge** su TikTok (dicembre 2022), dove l’effetto filtro “invisibile” è stato usato per adescare vittime. Ricercatori Bitdefender e Checkmarx hanno osservato che creatori di contenuti pubblicavano video virali invitando gli utenti a

scaricare un’app *“che rimuove il filtro invisibile”*.

I video, con oltre un milione di visualizzazioni in pochi giorni, reindirizzavano le vittime a un server Discord: qui si sosteneva di mostrare *video “svelati”*, ma in realtà i link conducevano all’installazione di **Wasp Stealer**, un trojan information-stealer noto per rubare password, dati di carte di credito e criptovalute. In questo scenario l’attacco era orchestrato come un *una truffa di social engineering*: gli utenti incuriositi dai video – molti dei quali mostrano i protagonisti privi di vestiti – venivano convinti che una app “speciale” avrebbe rivelato contenuti segreti, ma scaricavano malware al posto di una app legittima.

Altri report evidenziano minacce correlate: ad esempio un’analisi di Cofense ha mostrato come gli **URL di TikTok** vengano talvolta usati in campagne di phishing. In questi casi i criminali inseriscono link TikTok (ad es. nella bio di un profilo) che reindirizzano a siti maligni. L’obiettivo è sfruttare la fiducia degli utenti nel dominio ufficiale TikTok: “gli aggressori aggirano così i sospetti dell’utente e sfruttano la fiducia che molti ripongono nella piattaforma”. In sintesi, la condivisione di link dannosi o contenuti creativi infetti su TikTok è già stato registrato come vettore di trojan e phishing, e mostra quanto l’ecosistema social sia oggi oggetto di nuovi vettori di attacco.

Meccanismi di diffusione dei video virali TikTok e social engineering

I video virali su TikTok possono fungere da **vettore di attacco** sfruttando soprattutto l’ingegneria sociale. Gli attaccanti creano contenuti apparentemente innocui – tutorial per trucchi, sfide di tendenza o offerte *too-good-to-be-true* – per catturare l’attenzione. All’interno del video il malintenzionato istruisce verbalmente l’utente a compiere azioni tecniche: ad esempio aprire il prompt dei comandi o

PowerShell e incollare un comando.

Questa istruzione, presentata come passaggio necessario per attivare funzionalità premium, in realtà scarica uno script dannoso da un server remoto. Poiché **il codice non è presente nel video ma viene eseguito dall'utente**, le normali difese antivirus sul dispositivo dell'utente non intercettano nulla su TikTok stesso. Come spiega Trend Micro, "nessun codice malevolo è visibile sulla piattaforma che possa essere analizzato o bloccato da soluzioni di sicurezza" – tutta l'azione malevola avviene attraverso la persuasione diretta del video.

Oltre agli script PowerShell, gli aggressori possono inserire **link dannosi** nei commenti, nelle descrizioni o nelle biografie. Ad esempio, i profili possono contenere URL abbreviati o TikTok.link che, se cliccati, reindirizzano a siti di phishing o download di trojan. Cofense ha evidenziato casi in cui messaggi di posta phishing utilizzavano URL di TikTok per mimetizzare il redirect verso pagine di raccolta credenziali. In questo modo l'utente viene convinto di visitare una risorsa affidabile anche quando in realtà viene spinto verso trappole malware.

Steganografia e occultamento: in teoria, contenuti multimediali (immagini, audio, video) possono nascondere informazioni malevole tramite tecniche di steganografia. Per esempio, un aggressore potrebbe impercettibilmente incorporare istruzioni o payload in un video o nella sua traccia audio. In ambito accademico si studiano già "schemi robusti di video steganography" per comunicazioni segrete su social media.

In pratica, ciò significa che un video virale potrebbe avere dati cifrati incorporati nei frame: un malware o uno script sarebbe estratto dall'audio/video su dispositivo vittima. Sebbene non vi siano casi pubblici noti di steganografia specifica su TikTok, i ricercatori segnalano che **i social network basati su video offrono un mezzo ideale per**

comunicazioni occultate. La popolarità del mezzo (e la ridondanza delle trasmissioni video compressi) può mascherare segmenti di dati malevoli difficili da rilevare con analisi convenzionali.

In sintesi, i video virali favoriscono la diffusione di malware per due ragioni chiave: il **fattore psicologico** (utente rilassato e ingannato dalla natura di "intrattenimento" del contenuto) e la **portata algoritmica** di TikTok. L'algoritmo favorisce la viralità dei contenuti più popolari, amplificando i video malevoli fino a centinaia di migliaia di visualizzazioni. Gli attaccanti possono quindi dirigere i propri contenuti a segmenti specifici (es. paesi, fasce d'età) grazie agli strumenti di targeting di TikTok, rendendo l'attacco altamente scalabile. L'uso crescente di **contenuti generati da IA** (voci sintetiche, avatar faceless) permette di automatizzare la creazione di varianti di video malevoli, rendendo più agevole bombardare la piattaforma con nuovi video fraudolenti.

Contromisure e suggerimenti per gli utenti

Per proteggersi, gli utenti devono adottare precauzioni sia comportamentali che tecniche. Innanzitutto, **la scetticismo è fondamentale**: diffidate di video che promettono "software gratis", trucchi facili o filtri miracolosi. Non seguire ciecamente istruzioni di "esperti sconosciuti". Qualunque offerta di attivare Windows, Office, Spotify, CapCut o rimuovere filtri TikTok tramite passaggi complessi dovrebbe suonare come un potenziale inganno. Bitdefender raccomanda di «scrutare attentamente» qualsiasi rivendicazione riguardo alla rimozione di filtri o sblocchi TikTok e di **attivare l'autenticazione a due fattori** (2FA) quando possibile.

Dal punto di vista tecnico, tenete il sistema operativo e il software di sicurezza aggiornati. Installate un antivirus o

soluzione antimalware affidabile; questa può rilevare possibili payload scaricati. Evitate di scaricare app TikTok modificate o da fonti non ufficiali: usate sempre gli store ufficiali (Google Play, App Store) e verificate che l'app di TikTok stessa sia aggiornata e certificata. Disabilitate l'esecuzione automatica di script o codice scaricato via internet. Se un video istruisce ad aprire il prompt dei comandi o PowerShell, **non fatelo** – è una pratica insolitamente rischiosa. Anche Trend Micro consiglia di monitorare l'esecuzione di comandi insoliti: "Tenere sotto controllo esecuzioni anomale di PowerShell o altri strumenti di sistema aiuta a individuare attività malevole in anticipo".

Inoltre, prestare attenzione alle **registrazioni e ai link** condivisi su TikTok. Non cliccate su URL sospetti in commenti o biografie di profili sconosciuti. Se un link vi sembra breve o strano, usate uno strumento online per verificarne la destinazione prima di visitarlo. Per i genitori o educatori, controllare e limitare l'uso di TikTok su dispositivi condivisi e spiegare ai più giovani i rischi di installare software non verificato è una buona pratica. Infine, segnalate immediatamente alla piattaforma ogni video o account sospetto: TikTok dispone di funzioni di report e rimozione per contenuti fraudolenti o pericolosi.

In sintesi, la difesa si basa su **consapevolezza dell'utente** e su barriere tecniche. Continuare ad aggiornare le soluzioni di sicurezza, evitare link e comandi non richiesti, e mantenere alta la guardia sulle nuove tecnologie (es. contenuti IA) sono accorgimenti che riducono notevolmente il rischio di contrarre trojan o altri malware tramite video virali. Come avvertono gli analisti di sicurezza, rinforzare l'educazione alla sicurezza informatica e trattare con sospetto i video "miracolosi" su TikTok è cruciale per spegnere sul nascere queste campagne.

Fonti:

Bizgă A. (2022). *Malicious Actors Exploit TikTok ‘Invisible Challenge’ to Steal Users’ Info*. Bitdefender Labs.

Gatlan S. (2025). *TikTok videos now push infostealer malware in ClickFix attacks*. BleepingComputer.

Dela Cruz J. (2025). *TikTok Videos Promise Pirated Apps, Deliver Vidar and StealC Infostealers Instead*. Trend Micro Research.

Knop D. (2025). *Social engineering campaign: TikTok videos with malware instructions*. Heise Security.

Cook B., McLain B. (2024). *Exploiting Social Media: TikTok Links Used to Hijack Microsoft Accounts*. Cofense Blog.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/video-virali-tiktok/