



Kaspersky: 15 milioni di attacchi mascherati da VPN, soprattutto tra la GenZ

Descrizione

COMUNICATO STAMPA ?? CONTENUTO PROMOZIONALE

La Generazione Z utilizza gli strumenti per la privacy in modo più attivo rispetto a qualsiasi altra generazione, ma questa abitudine potrebbe anche renderla un bersaglio per i criminali informatici. Tra ottobre 2024 e settembre 2025, Kaspersky ha rilevato oltre 15 milioni di tentativi di attacco mascherati da applicazioni VPN. Invece di proteggere gli utenti, queste VPN false o crackate spesso distribuiscono malware e software potenzialmente indesiderati, che vanno dai downloader e dagli adware fino ai trojan capaci di rubare dati e garantire agli aggressori l'accesso remoto.

Secondo i risultati della ricerca, la GenZ utilizza VPN, strumenti di crittografia, navigazione in incognito e altre tecnologie per la protezione della privacy con una frequenza doppia rispetto alle fasce d'età maggiori. Essendo cresciuti nell'era delle fughe di dati, del tracciamento algoritmico e delle piattaforme social iperconnesse, sono molto più consapevoli di quanto la privacy online possa essere fragile. Le VPN e i browser anonimi sono quindi diventati strumenti essenziali per proteggere i dati personali, salvaguardare le identità digitali e garantire la sicurezza durante l'uso di Wi-Fi pubblici.

Ma questo cambiamento comporta un pericolo inaspettato: nella ricerca della sicurezza, molti giovani utenti potrebbero ricorrere ad applicazioni VPN gratuite, pirata o contraffatte, strumenti che in apparenza sembrano proteggerli ma che in realtà li espongono a rischi significativamente maggiori. Tra ottobre 2024 e settembre 2025, gli esperti di Kaspersky hanno infatti rilevato oltre 15 milioni di tentativi di attacco nascosti all'interno di diverse applicazioni VPN.

Nel periodo osservato, le minacce più comuni rivolte agli utenti sono state dominate da tre categorie di malware e software potenzialmente indesiderati. In cima alla lista si trova l'AdWare, con 284.261

casi, che continua a disturbare gli utenti attraverso annunci intrusivi, reindirizzamenti indesiderati e forme di tracciamento aggressivo. I trojan seguono da vicino con 234.283 rilevamenti, rappresentando un pericolo significativo per la loro capacità di rubare dati e consentire agli aggressori il controllo remoto completo dei sistemi compromessi. Le minacce di tipo downloader si sono invece classificate al terzo posto, con 197.707 casi rilevati, confermando il loro ruolo di punto di ingresso privilegiato per l'installazione di ulteriori payload dannosi sui dispositivi delle vittime.

I ricercatori di Kaspersky hanno anche identificato pagine di phishing che imitano i portali di accesso di noti servizi VPN. Questi siti inducono gli utenti a inserire le proprie credenziali, esponendoli al rischio di perdere l'accesso ai loro account VPN e, potenzialmente, a molti altri, se la stessa password viene riutilizzata su più piattaforme. Particolarmente significativo è il fatto che queste pagine di phishing risultino sorprendentemente simili tra loro, un dettaglio che suggerisce siano state generate tramite kit di phishing, strumenti che permettono agli aggressori di produrre in serie pagine fraudolente credibili e già pronte con il minimo sforzo.

La GenZ può essere attenta alla privacy, ma è anche pragmatica e spesso guidata dalla convenienza. Questo comportamento crea un'opportunità che i criminali informatici sfruttano attivamente. Gli aggressori possono infatti promuovere deliberatamente versioni pirata di servizi VPN premium e sviluppare app che imitano nome e design di brand noti nel campo della privacy. Di conseguenza, i giovani utenti che credono sinceramente di rafforzare la propria protezione online potrebbero, in realtà, consegnare l'accesso ai propri dispositivi e alle proprie informazioni personali direttamente agli aggressori. ha affermato Evgeny Kuskov, Security Expert di Kaspersky.

Per aiutare la Generazione Z ad affrontare le minacce digitali nel mondo dell'interattivismo, Kaspersky ha lanciato il gioco interattivo "Case 404", progettato per parlare la loro lingua. Il gioco permette ai partecipanti di immergersi in un mondo in cui download e offerte apparentemente innocue nascondono gravi rischi per la sicurezza informatica. Durante l'esperienza, gli utenti scoprono pericoli nascosti e imparano a proteggersi da malware, truffe e fughe di dati personali. Come ricompensa per aver completato il gioco, i partecipanti ricevono uno sconto esclusivo su Kaspersky Premium, che mette a loro disposizione strumenti affidabili per navigare in sicurezza nel mondo digitale.

Per proteggersi, Kaspersky raccomanda di:

Contatti:
Kaspersky

kaspersky@noesis.net

COMUNICATO STAMPA ?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Dicembre 1, 2025

Autore

redazione

default watermark