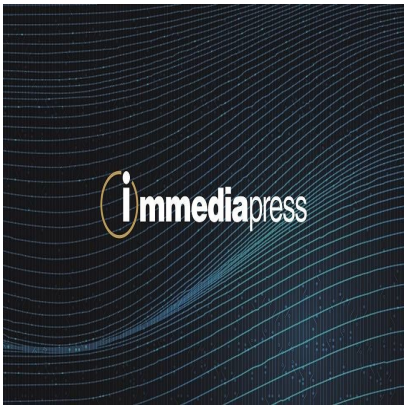

Sciando sul filo del rischio: Kaspersky svela le minacce informatiche da conoscere in occasione di un grande evento sportivo invernale

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

I giochi invernali del 2026 prenderanno il via il 6 febbraio in Italia, attirando lâ??attenzione di appassionati e tifosi sia online che offline. Centinaia di atleti parteciperanno allâ??evento e le cittÃ ospitanti accoglieranno un grande afflusso di pubblico. Gli esperti Kaspersky GReAT hanno individuato alcune delle principali minacce informatiche che possono emergere in occasione di un grande evento internazionale, indipendentemente dal luogo in cui si svolge.

Ransomware

Gli autori di attacchi ransomware, sempre alla ricerca del massimo profitto, possono considerare gli eventi di massa e le organizzazioni coinvolte, come fornitori e altre realtÃ della supply chain, come obiettivi di alto valore. Per ottenere il massimo profitto dallâ??elevata domanda di partecipazione in presenza, questi attacchi possono colpire le reti alberghiere delle cittÃ ospitanti, cosÃ¬ come stadi, piattaforme ufficiali di vendita dei biglietti e altre risorse digitali legate allâ??evento.

Attacchi APT

Anche i gruppi responsabili di attacchi APT (Advanced Persistent Threat) guardano ai grandi eventi internazionali come a obiettivi strategicamente rilevanti, grazie alla loro visibilitÃ globale, allâ??elevata concentrazione di societÃ appaltatrici di infrastrutture IT critiche e alla complessitÃ delle catene di fornitura coinvolte. Un esempio significativo Ã¨ rappresentato dal malware noto come Olympic Destroyer, impiegato contro lâ??infrastruttura IT durante lâ??evento sportivo di PyeongChang nel 2018. In quellâ??occasione, il malware si Ã¨ diffuso allâ??interno della rete degli organizzatori tramite

credenziali compromesse, con lâ??obiettivo di sabotare e interrompere il regolare svolgimento dellâ??evento.

â??Eventi di questa portata attirano inevitabilmente lâ??attenzione dei criminali informatici e le potenziali minacce possono assumere molte forme, colpendo spettatori, infrastrutture urbane e atleti, oltre a milioni di persone che accedono ai servizi digitali prima, durante e dopo lâ??evento. La dimensione internazionale e il vasto pubblico rendono questi contesti particolarmente appetibili per attori sofisticati, rappresentando minacce serie alle quali tutti i soggetti coinvolti dovrebbero essere preparatiâ?•, ha dichiarato Igor Kuznetsov, Director del Global Research & Analysis Team (GReAT).

Attacchi di hacktivismo

Gli hacktivisti possono avviare campagne mirate contro le organizzazioni coinvolte nellâ??evento per perseguire i propri obiettivi strategici e attirare lâ??attenzione dellâ??opinione pubblica. Queste operazioni possono tradursi in furti e fughe di dati, campagne di disinformazione o interruzioni dei sistemi chiave, come le infrastrutture di trasmissione o le piattaforme di vendita dei biglietti, con potenziali conseguenze sia per gli spettatori sia per le organizzazioni coinvolte.

Attacchi alle infrastrutture urbane

Sia gli attori mossi da motivazioni economiche sia altre tipologie di minacce possono prendere di mira i sistemi critici delle cittÃ , inclusi trasporti, servizi pubblici, reti di comunicazione e hotspot Wi-Fi pubblici vulnerabili, con lâ??obiettivo di interrompere i servizi o compromettere la stabilitÃ operativa. Secondo uno studio condotto da Kaspersky nel 2024, alla vigilia di un grande evento sportivo estivo tenutosi a Parigi, quasi il 25% dei circa 25.000 hotspot Wi-Fi gratuiti analizzati risultava avere una crittografia debole o assente, esponendo gli utenti al rischio di furto di dati personali e bancari.

Questi attacchi possono avvenire tramite malware, intrusioni di rete o manipolazione dei sistemi connessi, con possibili ripercussioni sui servizi cittadini da cui dipendono residenti e visitatori. Lâ??adozione di soluzioni di sicurezza, insieme allâ??uso di una VPN, puÃ² contribuire a proteggere i dati, crittografando la connessione Internet e tutelando lâ??attivitÃ online.

Attacchi agli atleti

I criminali informatici possono sfruttare le informazioni disponibili pubblicamente e la popolaritÃ degli atleti partecipanti. Tra gli scenari possibili figurano campagne di phishing mirate e operazioni basate su deepfake, finalizzate al furto di dati o al ricatto. Destano particolare preoccupazione anche il potenziale

dirottamento degli account social, il rischio di doxxing, ovvero la diffusione pubblica di informazioni private, e altre forme di abuso tecnologico che possono compromettere la sicurezza personale degli atleti.

Gli attori malevoli possono inoltre approfittare delle vulnerabilitÃ della sicurezza online, ad esempio attraverso fughe di dati che espongono informazioni personali degli utenti. La funzione Data Leak Checker di Kaspersky Premium consente di individuare eventuali compromissioni degli account, avvisando tempestivamente gli utenti in caso di rischi di esposizione.

Il pubblico come target

I giochi invernali attirano migliaia di persone nel Paese ospitante. Gli spettatori presenti sul posto possono incorrere in truffe come la vendita di biglietti falsi, con conseguente furto di denaro dai conti bancari o persino la compromissione delle credenziali dei portafogli di criptovalute, anzichÃ© lâ??accesso agli eventi desiderati. Parallelamente, i fan online possono essere esposti a live streaming falsi e a siti web fraudolenti che propongono merchandising contraffatto dei loro atleti preferiti.

I viaggiatori possono inoltre imbattersi in servizi ingannevoli che si presentano come piani tariffari per telefoni cellulari, ma che in realtÃ raccolgono e sottraggono informazioni personali e finanziarie. Per questo motivo, scegliere Kaspersky eSIM Store rappresenta una soluzione pratica per rimanere sempre connessi, evitando servizi fraudolenti e i disagi legati allâ??uso delle SIM fisiche.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Febbraio 3, 2026
Autore

redazione