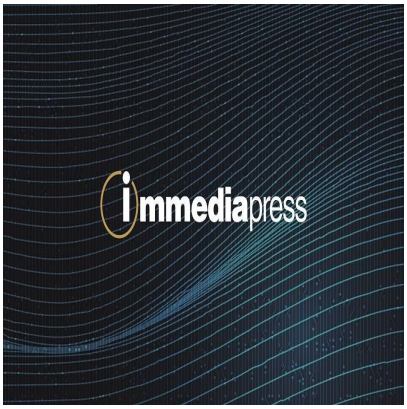

Kaspersky: nuova tecnica di phishing che sfrutta Bubble, piattaforma di IA senza codice

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Kaspersky ha individuato una nuova tecnica di phishing progettata per eludere i tradizionali controlli di sicurezza. Questa tecnica sfrutta Bubble, una piattaforma che consente di creare applicazioni web e mobile tramite unâ??interfaccia visiva, senza la necessitÃ di scrivere codice. Sempre piÃ¹ spesso, gli autori degli attacchi ricorrono a strumenti innovativi pensati per lo sviluppo di software legittimo, riutilizzandoli per rendere piÃ¹ efficaci le campagne di phishing.

I tradizionali attacchi di phishing si basano generalmente su link dannosi o su reindirizzamenti facilmente identificabili, che i moderni sistemi di sicurezza riescono spesso a intercettare e bloccare. Tuttavia, gli aggressori stanno ora sfruttando lâ??ambiente no-code di Bubble per creare applicazioni web intermedie, ospitate su infrastrutture legittime e su domini affidabili come *.bubble.io. Questo ne aumenta la credibilitÃ e consente di aggirare piÃ¹ facilmente i filtri di sicurezza. Tali applicazioni agiscono come reindirizzamenti nascosti, indirizzando silenziosamente le vittime verso siti dannosi progettati per sottrarre credenziali.

Nella campagna analizzata, le vittime venivano reindirizzate ripetutamente a una pagina di accesso Microsoft estremamente realistica, protetta da un ulteriore livello di verifica Cloudflare, pensato per nascondere ulteriormente le intenzioni malevole.

Ã? probabile che questa tecnica venga integrata in piattaforme piÃ¹ ampie di phishing-as-a-service (PhaaS) e nei kit di phishing. Questi strumenti offrono unâ??ampia gamma di funzionalitÃ dannose giÃ pronte allâ??uso, tra cui lâ??intercettazione in tempo reale dei cookie di sessione, la gestione di campagne di phishing tramite servizi legittimi come Google Tasks e Google Forms e lâ??esecuzione di

attacchi â??adversary-in-the-middleâ?• (AiTM), capaci di aggirare lâ??autenticazione a piÃ¹ fattori. Inoltre, supportano la generazione di e-mail di phishing tramite intelligenza artificiale, integrano meccanismi di geo-filtraggio e tecniche anti-rilevamento per eludere i sistemi di sicurezza, e sono spesso ospitati su servizi cloud affidabili come AWS per evitare di essere inseriti nelle blacklist.

â??Lâ??uso di piattaforme legittime come Bubble introduce un nuovo livello di abuso della fiducia, rendendo piÃ¹ difficile, sia per gli utenti sia per i sistemi automatizzati, distinguere tra contenuti sicuri e dannosi. Questo aumenta significativamente il rischio di furto di credenziali, accessi non autorizzati e possibili violazioni dei datiâ?•, ha commentato Roman Dedenok, Anti-Spam Expert di Kaspersky.

Per proteggersi da queste minacce, Kaspersky consiglia di:

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
Marzo 24, 2026
Autore
redazione