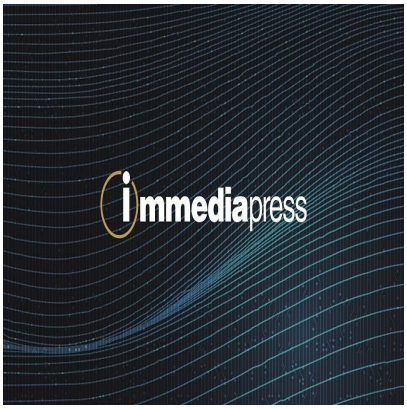

Kaspersky scopre una campagna infostealer su macOS che sfrutta funzioni di condivisione chat di ChatGPT

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Kaspersky Threat Research ha identificato una nuova campagna malware che sfrutta annunci di ricerca Google a pagamento e conversazioni condivise sul sito web ufficiale di ChatGPT per indurre gli utenti Mac a eseguire il comando che installa lâ??infostealer AMOS (Atomic macOS Stealer) e una backdoor persistente sui loro dispositivi.

Nella campagna, gli aggressori acquistano annunci di ricerca sponsorizzati per query come â??chatgpt atlasâ?• e indirizzano gli utenti a una pagina che sembra essere una guida allâ??installazione di â??ChatGPT Atlas per macOSâ?•, ospitata su chatgpt.com. In realtÃ , la pagina Ã¨ una conversazione ChatGPT condivisa, generata tramite prompt engineering e poi ripulita in modo da lasciare solo le istruzioni dettagliate per lâ??â??installazioneâ?•. La guida invita gli utenti a copiare una singola riga di codice, aprire Terminal su macOS, incollare il comando e concedere tutte le autorizzazioni richieste.

Lâ??analisi dei ricercatori di Kaspersky mostra che il comando scarica ed esegue uno script dal dominio esterno atlas-extension[.]com. Lo script richiede ripetutamente allâ??utente la password di Sistema e la convalida tentando di eseguire comandi di sistema. Una volta fornita la password corretta, lo script scarica lâ??infostealer AMOS, utilizza le credenziali rubate per installarlo e avvia il malware. Il flusso di infezione rappresenta una variante della cosiddetta tecnica ClickFix, in cui gli utenti vengono persuasi a eseguire manualmente comandi shell che recuperano ed eseguono codice da server remoti.

Dopo lâ??installazione, AMOS raccoglie dati che possono essere monetizzati o riutilizzati in successive intrusioni. Il malware prende di mira password, cookie e altre informazioni dai browser piÃ¹ diffusi, dati

dai portafogli di criptovalute come Electrum, Coinomi ed Exodus e informazioni da applicazioni quali Telegram Desktop e OpenVPN Connect. Cerca anche file con estensioni TXT, PDF e DOCX nelle cartelle Desktop, Documenti e Download, nonchÃ© file archiviati dallâ??applicazione Notes, quindi esfiltra questi dati verso unâ??infrastruttura controllata dallâ??autore dellâ??attacco. Parallelamente, lâ??attacco installa una backdoor configurata per avviarsi automaticamente al riavvio, che consente lâ??accesso remoto al sistema compromesso e duplica gran parte della logica di raccolta dati di AMOS.

La campagna riflette una tendenza piÃ¹ ampia in cui gli infostealer sono diventati una delle minacce in piÃ¹ rapida crescita del 2025, con gli aggressori che sperimentano attivamente temi legati allâ??intelligenza artificiale, strumenti di intelligenza artificiale falsi e contenuti generati dallâ??intelligenza artificiale per aumentare la credibilitÃ delle loro esche. Le recenti ondate hanno incluso barre laterali del browser AI false e client fraudolenti per modelli popolari; lâ??attivitÃ a tema Atlas estende questo modello abusando della funzione di condivisione dei contenuti integrata in una piattaforma AI legittima.

â??Quello che rende efficace questo caso non Ã¨ un exploit sofisticato, ma il modo in cui il social engineering Ã¨ inserito in un contesto familiare di intelligenza artificialeâ?•, ha affermato Vladimir Gursky, Malware Analyst di Kaspersky. â??Un link sponsorizzato porta a una pagina ben formattata su un dominio affidabile e la guida allâ??installazione Ã¨ costituita da un solo comando Terminal. Per molti utenti, questa combinazione di fiducia e semplicitÃ Ã¨ sufficiente per aggirare la loro consueta cautela, ma il risultato Ã¨ la compromissione totale del sistema e lâ??accesso a lungo termine per lâ??autore dellâ??attaccoâ?•.

Kaspersky raccomanda agli utenti 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
Dicembre 11, 2025
Autore
redazione