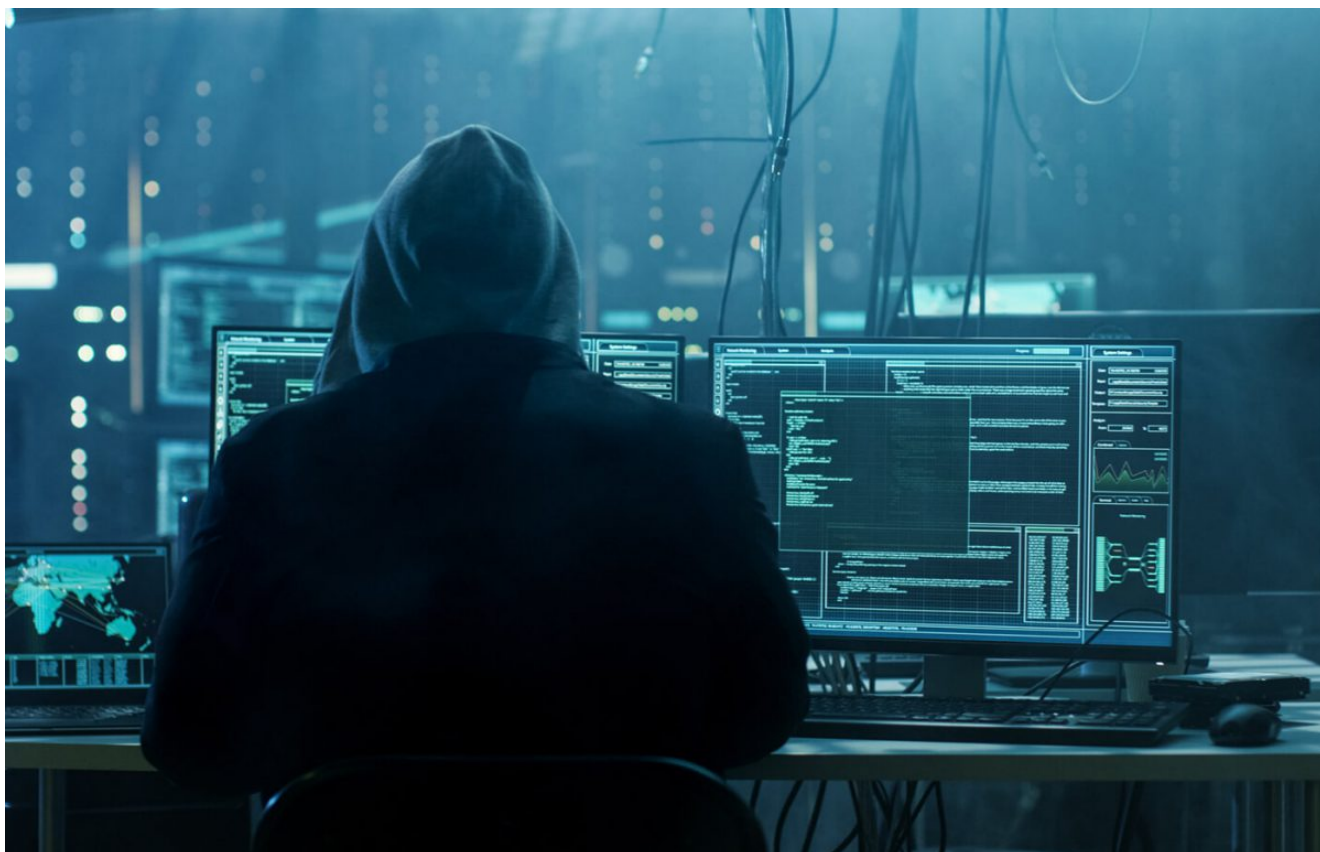


Cybercrime, negli ultimi 6 mesi del 2023 attacchi a tema AI e casi di spyware Android. Il report



Il secondo semestre del 2023 è stato caratterizzato da significativi incidenti di cybersicurezza. **Cl0p**, famigerato gruppo di criminali informatici noto per la realizzazione di attacchi ransomware su larga scala, ha attirato l'attenzione a causa delle estese attività di **"MOVEit hack"**, che sorprendentemente non hanno comportato la distribuzione di ransomware.

I dati si leggono l'ultimo Threat Report di ESET, che sintetizza le tendenze osservate dai sistemi di rilevamento e dagli esperti da giugno a novembre 2023.

Nel panorama IoT, i ricercatori hanno identificato un kill

switch che è stato utilizzato per rendere non funzionante la botnet IoT Mozi. Tra le discussioni prevalenti sugli attacchi abilitati all'intelligenza artificiale, ESET ha identificato campagne specifiche che prendono di mira gli utenti di strumenti come ChatGPT e l'API OpenAI. Per quanto riguarda lo spyware, si è registrato un aumento significativo dei casi di spyware Android, attribuito principalmente alla presenza della minaccia Spin0k.

Una nuova minaccia contro i dispositivi IoT, Android/Pandora, ha compromesso dispositivi Android – tra cui smart TV, TV box e dispositivi mobili – e li ha utilizzati per attacchi DDoS. ESET Research ha inoltre registrato un numero considerevole di tentativi di accesso a domini dannosi con nomi che assomigliano a “**ChatGPT**”, apparentemente in riferimento al chatbot ChatGPT. Le minacce riscontrate attraverso questi domini includono applicazioni web che gestiscono in modo non sicuro le chiavi **API OpenAI**, sottolineando l'importanza di proteggere la privacy dei codici degli utenti.

Tra le minacce Android, lo spyware **Spin0K**, distribuito come kit di sviluppo software, che si trova all'interno di varie applicazioni Android legittime. Su un altro fronte, la seconda minaccia più registrata nell'H2 2023 è il codice malevolo JavaScript rilevato come JS/Agent, che continua a essere introdotto in siti web compromessi.

Per contro, la crescita del valore dei bitcoin non è stata accompagnata da un corrispondente aumento delle minacce alle criptovalute, discostandosi dalle tendenze del passato. Tuttavia, i furti di criptovalute hanno registrato un notevole incremento, causato dalla diffusione del *malware-as-a-service infostealer* **Lumma Stealer**, che ha come obiettivo i portafogli di criptovalute.

Per approfondire

<https://www.key4biz.it/cybercrime-negli-ultimi-6-mesi-del-2023-attacchi-a-tema-ai-e-casi-di-spyware-android-il-report/473023/>