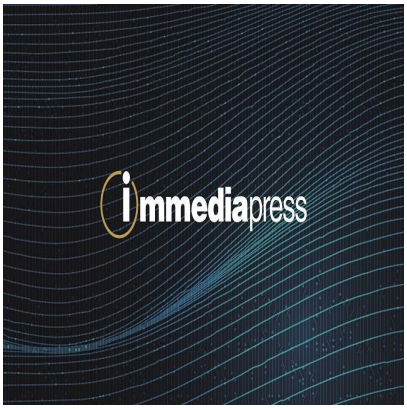

COMUNICATO STAMPA SPONSORIZZATO â?? Kaspersky: gli attacchi DLL hijacking sono raddoppiati dal 2023

Descrizione

(Immediapress) â??

Secondo Kaspersky negli ultimi due anni gli attacchi di tipo DLL hijacking sono raddoppiati. La versione aggiornata di Kaspersky SIEM Ã¨ ora dotata di funzionalitÃ AI per rilevare gli attacchi di tipo DLL hijacking, migliorando lâ??efficienza del rilevamento.

Milano, 06 ottobre 2025. Il DLL hijacking (â??Dynamic Link Library hijackingâ?•) Ã¨ una tecnica comune con cui gli attaccanti sostituiscono la libreria caricata da un processo legittimo con unâ??altra dannosa. Questa tecnica viene utilizzata sia dai creatori di malware ad alto impatto, come stealer e trojan bancari, sia da gruppi APT (Advanced Persistent Threat) e cybercriminali che si occupano di attacchi mirati.

Kaspersky ha rilevatoquesta tecnica e le sue varianti, come il sideloading delle DLL, durante alcuni attacchi mirati contro diverse aziende in Russia, Africa, Corea del Sud e altre regioni. Per migliorare ancora di piÃ¹ la protezione contro questa minaccia, Kaspersky SIEM ha aggiunto un nuovo sottosistema basato sullâ??intelligenza artificiale che controlla sempre le informazioni relative a tutte le librerie caricate.

Questa nuova funzionalitÃ ha giÃ dimostrato la sua efficacia, aiutando a rilevare un attacco da parte del gruppo APT ToddyCat. La minaccia Ã¨ stata identificata e bloccata in una fase iniziale, evitando qualsiasi impatto sulle aziende prese di mira. Il modello ha anche rilevato dei tentativi per infettare potenziali vittime con un infostealer e un loader dannoso.

â??Stiamo assistendo a un aumento degli attacchi DLL hijacking, in cui un programma affidabile viene indotto a caricare una libreria falsa invece di quella reale. Questo consente agli aggressori di eseguire segretamente il loro codice dannoso. Questa tecnica Ã¨ difficile da rilevare, ed Ã¨ qui che lâ??intelligenza artificiale puÃ² essere dâ??aiuto. Lâ??utilizzo di tecniche di protezione avanzate potenziate dallâ??intelligenza artificiale Ã¨ ormai essenziale per stare al passo con queste minacce in continua evoluzione e mantenere sicuri i sistemi criticiâ?•,ha affermato Anna Pidzhakova, Data Scientist del Kaspersky AI Research Center.

Su Securelist sono stati pubblicati due articoli correlati: il primo spiega come Ã¨ stato sviluppato un modello di machine learning per rilevare gli attacchi di DLL hijacking, mentre il secondo descrive come questo modello sia stato integrato nella piattaforma SIEM di Kaspersky.

Ulteriori informazioni sul Kaspersky SIEM sono disponibili al seguente sito web.

Seguici su:

Tweets by KasperskyLabIT

http://www.facebook.com/kasperskylabitalia

https://www.linkedin.com/company/kaspersky-lab-italia

https://t.me/KasperskyItalia

Informazioni su Kaspersky

Kaspersky Ã¨ unâ??azienda globale di cybersecurity e privacy digitale fondata nel 1997. Con oltre un miliardo di dispositivi protetti dalle minacce informatiche emergenti e dagli attacchi mirati, la profonda esperienza di Kaspersky in materia di sicurezza e di Threat Intelligence si trasforma costantemente in soluzioni e servizi innovativi per la sicurezza di aziende, infrastrutture critiche, governi e consumatori in tutto il mondo. Il portfolio completo dellâ??azienda comprende una protezione Endpoint leader, prodotti e servizi di sicurezza specializzati e soluzioni Cyber Immune per contrastare le minacce digitali

sofisticate e in continua evoluzione. Aiutiamo oltre 200.000 aziende a proteggere ciÃ² che piÃ¹ conta per loro. Per ulteriori informazioni Ã¨ possibile consultare https://www.kaspersky.it/

Contatti:
Immediapress
Contatto di redazione:
NoesisKaspersky Italia
kaspersky@noesis.net

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Ottobre 6, 2025
Autore
redazione