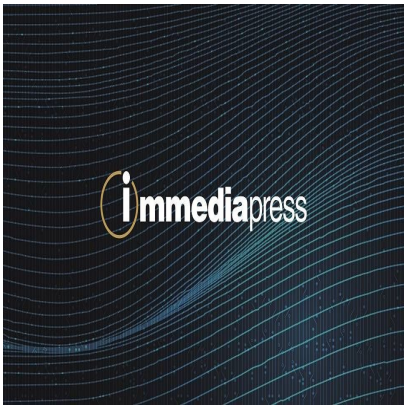

COMUNICATO STAMPA SPONSORIZZATO â?? Kaspersky: nuovi dettagli sullâ??attacco al worm NPM Shai-Hulud

Descrizione

(Immediapress) â?? Milano, 25 settembre 2025. Kaspersky Threat Research ha analizzato il pacchetto patient zero del worm Shai-Hulud, scoprendo come questo malware autoreplicante sia riuscito a lanciare un attacco alla supply chain dellâ??ecosistema NPM. Da una recente ricerca di Kaspersky, il worm Shai-Hulud ha infettato 190 pacchetti unici su un totale di 530 versioni, il che significa che molti pacchetti avevano piÃ¹ versioni violate durante lâ??attacco.

Il worm Shai-Hulud, un malware autoreplicante rivelato per la prima volta il 15 settembre 2025, si diffonde automaticamente attraverso gli account degli sviluppatori attraverso il furto di token di autenticazione e la pubblicazione di versioni infette di pacchetti legittimi. Sebbene lâ??impatto dellâ??attacco sia stato largamente documentato, lâ??analisi di Kaspersky rivela dettagli tecnici sui meccanismi di infezione iniziali e sui sofisticati metodi di diffusione del worm.

Le ricerche condotte da Kaspersky confermano che la versione 18.1.4 di ngx-bootstrap Ã¨ stata il pacchetto â??patient zeroâ?• e spiegano imetodi tecnici degli obiettivi raggiunti. I ricercatori hanno individuato una caratteristica distintiva fondamentale: mentre tutti i pacchetti infetti successivi eseguivano il codice dannoso tramite script post-installazione, il pacchetto â??patient zeroâ?• utilizzava in modo univoco un comando pre-installazione, rivelandosi il punto di partenza piuttosto che una vittima della diffusione automatizzata.

Il worm contiene funzionalitÃ progettate specificamente per compromettere i repository privati delle organizzazioni su GitHub. Oltre a rubare i token di autenticazione, il worm migra automaticamente i repository privati e interni da account GitHub aziendali agli utenti, rendendo di fatto accessibile al

pubblico il codice aziendale riservato ed esponendo interi codici proprietari.

â??La nostra analisi fornisce informazioni fondamentali sulle modalitÃ operative di questo attacco alla supply chain e sulla reale portata dellâ??esposizione dei repositoryâ?•, ha affermato Vladimir Gurskiy, Malware Analyst del Kaspersky Threat Research.â??La migrazione sistematica del worm repository privato dagli account aziendali a quelli personali rappresenta una significativa escalation delle minacce alla supply chain, che potrebbero esporre anni di lavoro di sviluppo proprietario. Questa ricerca conferma il motivo per cui continuiamo a gestireil Kaspersky Open Source Software Threats Data Feed: le aziende hanno bisogno di informazioni in tempo reale sui pacchetti compromessi per proteggere le loro pipeline di sviluppo proprio da questo tipo di attacchi sofisticatiâ?•.

Le soluzioni Kaspersky identificano il malware come HEUR:Worm.Script.Shulud.gen. Le aziende possono verificare la presenza di infezioni cercando â??shai-huludâ?• nei propri repository GitHub o la presenza di file shai-hulud-workflow.yml.

Maggiori informazioni sono disponibili su Securelist.

Kaspersky aveva giÃ segnalato la crescente tendenza degli attacchi alla supply chain che prendono di mira gli ecosistemi open source. I ricercatori dellâ??azienda hanno identificato la creazione di moduli dannosi come un vettore di attacco sempre piÃ¹ diffuso tra gli autori delle minacce.

Kaspersky Threat Research

Il team Threat Research Ã¨ leader nella protezione contro le minacce informatiche. Impegnato attivamente sia nellâ??analisi delle minacce che nella creazione di tecnologie, gli esperti di TR assicurano che le soluzioni di cybersecurity di Kaspersky siano costantemente informate e eccezionalmente potenti, in grado di fornire informazioni essenziali sulle minacce e una protezione solida per i nostri clienti e per la community in generale.

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/

Seguici su:

Tweets by KasperskyLabIT

http://www.facebook.com/kasperskylabitalia

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

https://www.instagram.com/kasperskylabitalia/

https://t.me/KasperskyItalia

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

Immediapress non sono responsabili per i contenuti dei comunicati trasmessi

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Settembre 26, 2025
Autore
redazione