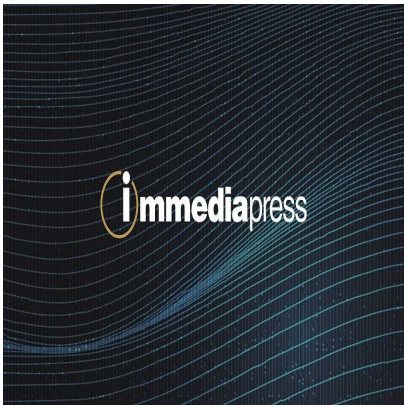

Attacchi al settore automotive: Kaspersky identifica i rischi nel 2026

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Le auto moderne sono diventate dispositivi digitali sempre piÃ¹ complessi, dotati di ampie capacitÃ di comunicazione remota e soggetti ad attacchi dannosi che possono colpire non solo i veicoli stessi, ma anche i sistemi a cui sono collegati. In questo contesto, Kaspersky condivide le proprie previsioni sulle minacce informatiche per lâ??industria automotive nel 2026.

Attacchi alle infrastrutture delle case automobilistiche

Nel 2026 continueranno gli attacchi da parte di malintenzionati motivati da ragioni finanziarie, che utilizzeranno principalmente ransomware. Lâ??obiettivo di tali attacchi Ã¨ crittografare file, sistemi o intere reti delle vittime, rendendoli inaccessibili, per poi richiedere il pagamento di un riscatto (solitamente in criptovaluta) in cambio della chiave di decrittografia o del ripristino dellâ??accesso. Potrebbero inoltre emergere nuove fughe di dati riservati degli utenti e informazioni sui movimenti dei veicoli provenienti dalle infrastrutture delle case automobilistiche.

Un altro vettore significativo Ã¨ rappresentato dagli attacchi alla supply chain delle infrastrutture delle case automobilistiche attraverso lâ??hacking dei sistemi degli appaltatori, con lâ??obiettivo di interrompere i sistemi critici e causare perdite finanziarie. Gli audit di sicurezza condotti regolarmente da Kaspersky consentono di identificare le vulnerabilitÃ che potrebbero essere sfruttate per questi attacchi.

Attacchi alle infrastrutture e alle flotte di taxi, ai servizi di car sharing, alle aziende di trasporto e logistica

Furto di dati personali e interruzione di sistemi critici. Gli aggressori motivati da ragioni finanziarie sono principalmente interessati ai dati personali degli utenti e allâ??accesso ai loro account. Sono possibili anche attacchi ransomware volti a interrompere sistemi critici e causare perdite economiche alle aziende.

Blocco remoto delle auto. Si tratta di un rischio particolarmente elevato, poichÃ© le societÃ di car sharing e taxi installano nei propri veicoli moduli che consentono, tra le altre funzioni, il blocco remoto in qualsiasi momento. Se gli aggressori ottengono lâ??accesso al sistema di controllo di questi moduli, possono bloccare simultaneamente numerosi veicoli, ad esempio per richiedere un riscatto o per effettuare operazioni di sabotaggio.

Hacking dei sistemi delle aziende di trasporto e logistica e intercettazione dei carichi. Un ulteriore potenziale vettore di rischio riguarda gli attacchi alle aziende di trasporto e logistica finalizzati allâ??intercettazione degli ordini e al furto fisico dei carichi. Nel contesto attuale, la digitalizzazione dei processi della supply chain consente agli aggressori di sottrarre carichi senza lasciare il cyberspazio. Gli attaccanti possono infatti violare i sistemi da remoto e manipolare i dati di spedizione per far consegnare i carichi a indirizzi specifici, destinati alla successiva rivendita.

Attacchi alle infrastrutture di rifornimento carburante e alle stazioni di ricarica per veicoli elettrici

La crescente digitalizzazione coinvolge anche le infrastrutture di rifornimento. Le moderne stazioni di servizio e le stazioni di ricarica per veicoli elettrici sono progettate per essere collegate a infrastrutture cloud, ampliando le opportunitÃ di attacco per gli hacker. Entro il 2026 potrebbero verificarsi attacchi a queste infrastrutture cloud con lâ??obiettivo di sottrarre carburante o elettricitÃ , nonchÃ© dati dei clienti, come informazioni personali o dettagli delle carte carburante.

Sfruttare i punti deboli dellâ??architettura delle auto per rubarle

La produzione globale di veicoli moderni e altamente computerizzati, dotati di numerose unitÃ di controllo elettronico (ECU), Ã¨ in costante aumento. Gli hacker continueranno quindi a sfruttare errori di implementazione e vulnerabilitÃ per sottrarre veicoli. Un esempio recente riguarda alcuni attaccanti

che sono riusciti a connettersi al bus CAN dei veicoli di un importante produttore attraverso un faro, ottenendo cosÃ¬ lâ??accesso al sistema di avviamento del motore. Gli esperti prevedono che nel 2026 verranno individuate nuove vulnerabilitÃ sfruttabili per il furto di automobili. I punti di accesso possono includere qualsiasi interfaccia accessibile, come bus CAN, porta OBD, porta Ethernet, modulo NFC, chip Wi-Fi e Bluetooth e modem LTE.

â??Ã? importante sottolineare che alcune case automobilistiche hanno iniziato a concentrarsi sulla sicurezza informatica, dimostrando un elevato senso di responsabilitÃ e preparandosi attivamente ad affrontare unâ??ampia gamma di minacce. Lavoriamo a stretto contatto con queste aziende, conducendo regolarmente audit di sicurezza su loro richiesta e contribuendo cosÃ¬ ad aumentare il livello di sicurezza lungo lâ??intera supply chain, dai produttori agli utenti finaliâ?•, ha commentato Artem Zinenko, Head di Kaspersky ICS Computer Emergency Response Team Vulnerability Research and Assessment.

I moderni sistemi informatici integrati nei veicoli sono collegati direttamente o indirettamente a Internet, rendendo gli attacchi contro di essi una questione di tempo. Per creare sistemi resistenti agli attacchi, Ã¨ necessario integrare i principi di sicurezza fin dalle fasi di progettazione e sviluppo, cosÃ¬ da mitigare alcuni rischi e ridurre al minimo la probabilitÃ di sfruttamento. Kaspersky ha sviluppato una propria soluzione per garantire la sicurezza delle informazioni dei veicoli: Kaspersky Automotive Secure Gateway, basata sul sistema operativo KasperskyOS. Inoltre, Ã¨ possibile ridurre i rischi effettuando controlli di sicurezza regolari per identificare e correggere tempestivamente le vulnerabilitÃ , nonchÃ© installando soluzioni specializzate con protezione contro ransomware e altri tipi di malware sugli endpoint delle reti aziendali e industriali.

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

Febbraio 11, 2026
Autore
redazione