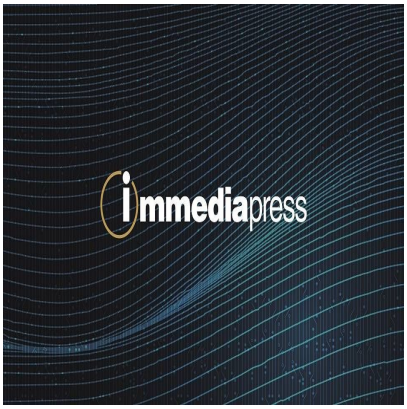

Cybersecurity industriale: i trend 2025 e le minacce attese nel 2026 secondo Kaspersky

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Il 2025 Ã¨ stato caratterizzato da una pressione costante sugli ambienti industriali, che ha trovato riscontro in un quadro di minacce globali sempre piÃ¹ complesso. Secondo il nuovo report Kaspersky Security Bulletin, la percentuale di computer ICS attaccati da malware Ã¨ rimasta elevata, attestandosi intorno al 21,9% nel primo trimestre, per poi scendere al 20% nel terzo trimestre. CiÃ² dimostra i progressi compiuti in termini di sicurezza informatica da parte delle organizzazioni, nonostante le tattiche degli aggressori siano in continua evoluzione. Si registrano disparitÃ a livello regionale, con Africa, Sud-Est asiatico, Asia orientale, Medio Oriente e Asia meridionale che registrano le percentuali piÃ¹ elevate di dispositivi ICS attaccati.

Minacce per settore industriale

I settori industriali hanno subito attacchi in misura diversa: al primo posto si colloca quello della biometria, con il 27,4% dei computer ICS con oggetti dannosi bloccati, seguito da building automation (23,5%), energia elettrica (21,3%), edilizia (21,1%), ingegneria e integrazione OT (21,2%), manifatturiero (17,3%) e oil & gas (15,8%). Queste cifre dimostrano che tutti i settori critici rimangono obiettivi primari per gli autori delle minacce.

Principali tendenze nei cyberattacchi alle realtÃ industriali

Gli aggressori hanno intensificato ulteriormente il ricorso ad attacchi alla supply chain e alle relazioni di fiducia, sfruttando fornitori locali, collaboratori esterni e provider di servizi mission-critical come gli

operatori di telecomunicazioni, per aggirare i tradizionali sistemi di difesa. Gli attacchi basati sullâ??intelligenza artificiale hanno registrato una forte espansione, dallâ??uso dellâ??IA come copertura per il malware alle operazioni di intrusione autonome guidate da agent. Si Ã¨ osservata unâ??ulteriore crescita degli attacchi alle apparecchiature OT connesse a Internet, in particolare ai siti remoti che si affidano a firewall OT non progettati per resistere alle moderne minacce provenienti da Internet.

Previsioni per il 2026

Il 2026 vedrÃ molto probabilmente un aumento degli incidenti che causeranno interruzioni nella logistica globale e nelle supply chain high-tech, insieme a un aumento degli attacchi contro obiettivi non tradizionali come i sistemi di trasporto intelligenti, le navi, i treni, i mezzi di trasporto pubblico, gli smart building e le comunicazioni satellitari. Si prevede che gli autori delle minacce, tra cui APT, gruppi regionali, hacktivisti e gang di ransomware, sposteranno sempre piÃ¹ le loro attivitÃ verso lâ??Asia, il Medio Oriente e lâ??America Latina, mentre le operazioni basate su agent AI e i framework di orchestrazione autonoma dannosa abbasseranno le barriere per le campagne industriali su larga scala.

â??Le aziende del settore industriale si trovano ad affrontare un contesto in cui gli attacchi sono piÃ¹ rapidi, intelligenti e asimmetrici che mai. Solo questâ??anno abbiamo analizzato campagne come Salmon Slalom, che ha preso di mira aziende del settore manifatturiero, delle telecomunicazioni e della logistica tramite phishing avanzato e sideloading di DLL, e lâ??operazione di spionaggio Librarian Ghouls, che ha compromesso istituti di ingegneria e ambienti di progettazione industriale. Questi attacchi dimostrano che sia le supply chain multinazionali che gli ecosistemi tecnici locali sono a rischio, e ogni azienda industriale deve ritenersi giÃ un bersaglio e agire di conseguenzaâ?•, ha dichiarato Evgeny Goncharov, Head of Kaspersky Industrial Control Systems Cyber Emergency Response Team.

Per proteggere i computer OT da varie minacce, Kaspersky ICS consiglia 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 18, 2025
Autore
redazione