

Toyota: un attacco ransomware costringe a fermare la produzione



Ancora una volta un **ransomware** colpisce il settore del **manufacturing**: vittima del cyber attacco un importante fornitore della famosa **Toyota**, la Kojima Industries, che ha rischiato di infettare direttamente i **sistemi IT** e **OT** della casa produttrice di automobili, insieme a tutte le altre aziende collaboratrici. Gli esperti di sicurezza lanciano l'allarme: i danni avrebbero potuto essere anche maggiori poiché l'intera infrastruttura non era debitamente protetta.

Danni provocati dal ransomware

L'attacco ha portato all'**arresto di 28 catene di produzione** distribuite su **14 fabbriche** nel territorio giapponese. Con l'interruzione della produzione per tutta la giornata di martedì, si stima che il colosso automobilistico giapponese abbia subito **perdite per circa 13.000 automobili**. La Toyota utilizza il metodo di fabbricazione del **Just-in-time**, che non prevede scorte di pezzi in magazzino.

Vulnerabilità della catena di produzione

La **Kojima Industries**, fornitore principale delle componenti plastiche per la Toyota, ha riscontrato la presenza di un virus insieme ad una richiesta di riscatto in lingua inglese dopo aver riavviato i server in seguito ad un errore riscontrato nella giornata di sabato scorso.

Non si conosce al momento l'autore o la motivazione dietro l'attacco, che ha portato alla luce evidenti vulnerabilità nella *production chain* giapponese. Sempre più spesso, essendo

le grandi aziende del calibro di Toyota ben equipaggiate in campo di cyber security, gli hacker tendono a colpire i loro subappaltatori di piccolo o medio livello, che vengono utilizzati come porte di accesso verso la grande industria. Il perimetro di attacco risulta molto esteso, considerando che la Toyota fa affidamento su circa 60.000 aziende fornitrici.

Il manufacturing sotto attacco ransomware

Secondo diversi report, il settore manifatturiero è stato il più colpito da attacchi ransomware nell'ultimo anno. Spesso le aziende non riescono a tenere sotto controllo tutte le centinaia o migliaia di dispositivi connessi on site. Sotto esame soprattutto i macchinari più vecchi, che non vengono sostituiti per motivi economici e che non riescono ad installare *patch* di aggiornamento perché l'azienda non può permettersi il *downtime*.

La Toyota ha affermato di essere riuscita a ripristinare l'operatività grazie a una rete di back-up condivisa con il fornitore, e ritiene che ci vorranno dalle 2 alle 3 settimane per tornare alla normale attività.

Il ransomware ha colpito anche **Hino Motors** e **Daihatsu Motor Co**, affiliati della Toyota.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/toyota-un-attacco-ransomware-costringe-a-fermare-la-produzione/>