Polimerica
Attualità e notizie dal mondo della plastica

Anche i computer industriali sotto attacco

Secondo una ricerca di Kaspersky Lab il 40% delle macchine è stato sottoposto ad un cyber attacco nella seconda metà del 2016.

6 aprile 2017 07:50

Solitamente si pensa che i computer industriali, quelli che sovrintendono a processi manifatturieri e non amministrativi, siano difficilmente attaccabili dall'esterno, poiché raramente collegati direttamente a Internet. Dimenticando però che queste macchine sono spesso collegate a PC connessi a Internet, questi ultimi potenzialmente vulnerabili; si tratta di computer gestiti da amministratori di sistema e di rete, sviluppatori e integrator di sistemi di automazione industriale e contractor di terze parti che si connettono alle reti tecnologiche direttamente o da remoto.

ATTACCATI 2 ICS SU 5. Secondo uno studio condotto da uno dei principali fornitori di sistemi contro le intrusioni informatiche, Kaspersky Lab ("Threat Landscape for Industrial Automation Systems in the second half of 2016"), nella seconda metà dell'anno scorso all'interno dell'infrastruttura tecnologica delle imprese industriali mediamente due ICS (Industrial Control Systems) su cinque sono stati sottoposti ad un attacco informatico. Le tre principali fonti d'infezione rilevate dai ricercatori sono Internet, i dispositivi di archiviazione rimovibili, gli allegati nocivi e il testo delle email.
Gli specialisti dell'ICS CERT (Industrial Control Systems Cyber Emergency Response Team) di Kaspersky Lab hanno scoperto che sono stati bloccati download di malware e tentativi di accesso a siti di phishing su oltre il 22% dei computer industriali. Questo significa che quasi una macchina su cinque ha rischiato l'infezione o la compromissione delle credenziali su internet almeno una volta.
Nel corso della ricerca sono stati individuati circa 20.000 diversi campioni di malware nei sistemi di automazione industriale appartenenti a oltre 2.000 differenti famiglie di malware; i tre Paesi con la maggiore percentuale di computer industriali attaccati sono stati Vietnam (oltre il 66%), Algeria (più di 65%) e Marocco (60%).

ANCHE CHIAVETTE ED E-MAIL. Internet non è però l'unica minaccia alla sicurezza informatica dei sistemi ICS, ci sono anche i dispositivi d'archiviazione rimovibili infetti. Durante il periodo analizzato, il 10,9% dei computer con software ICS installati (o connessi a dispositivi con questi software) hanno mostrato tracce di malware dopo la connessione di un dispositivo rimovibile.
Gli allegati nocivi e il testo delle email sono stati bloccati nell'8,1% dei computer industriali,

ottenendo la terza posizione nella classifica dei rischi per l'integrità dei dati. Nella maggior parte dei casi, i criminali hanno utilizzato email di phishing per attirare l'attenzione degli utenti e mascherare file nocivi.

IL FATTORE UMANO. I malware sono stati principalmente diffusi sotto forma di documenti Office o PDF. Usando diverse tecniche, i cyber criminali riescono a convincere le persone a scaricare e avviare i malware sui computer dell'azienda. "La nostra analisi mostra che confidare solamente nell'isolamento da internet delle reti tecnologiche non funziona più - commenta Evgeny Goncharov, Head of Critical Infrastructure Defense Department di Kaspersky Lab. - L'aumento delle cyber minacce per le infrastrutture critiche implica che gli ICS dovrebbero essere correttamente protetti dai malware sia all'esterno sia all'interno del perimetro. È inoltre importante notare che, secondo il nostro studio, gli attacchi iniziano quasi sempre dall'anello più debole della protezione: le persone".